Secure Access

Define Network Devices in Cisco ISE

A network device, such as a switch or a router, is an authentication, authorization, and accounting (AAA) client that sends AAA service requests to Cisco ISE. Defining network devices in Cisco ISE enables interactions between Cisco ISE and network devices.

Configure network devices for RADIUS or TACACS AAA, and Simple Network Management Protocol (SNMP) for the Profiling service to collect Cisco Discovery Protocol and Link Layer Discovery Protocol (LLDP) attributes for profiling endpoints, and TrustSec attributes for Cisco TrustSec devices. A network device that is not defined in Cisco ISE cannot receive AAA services from Cisco ISE.

From the Cisco ISE main menu, choose **Administration** > **Network Resources** > **Network Devices**, and click **Add**. In the **New Network Device** window that is displayed, enter the following details to define a network device:

- Select the vendor profile that fits the network device. The profile includes predefined configurations for the device, such as settings for URL redirect and change of authorization.

- Configure the RADIUS protocol for RADIUS authentications. When Cisco ISE receives a RADIUS request from a network device, it looks for the corresponding device definition to retrieve the configured shared secret. If Cisco ISE finds the device definition, it obtains the configured shared secret on the device and matches it against the shared secret in the request to authenticate access. If the shared secrets match, the RADIUS server processes the request further based on the policy and configuration. If the shared secrets do not match, a reject response is sent to the network device. A failed authentication report is generated, which provides the failure reason.

- Configure the TACACS+ protocol for TACACS+ authentications. When Cisco ISE receives a TACACS+ request from a network device, it looks for the corresponding device definition to retrieve the shared secret that is configured. If it finds the device definition, it obtains the shared secret that is configured on the device and matches it against the shared secret in the request to authenticate access. If the shared secrets match, the TACACS+ server processes the request further based on the policy and configuration. If they do not match, a reject response is sent to the network device. A failed authentication report is generated, which provides the failure reason.

- You can configure the Simple Network Management Protocol (SNMP) in the network device definition for the Profiling service to communicate with the network devices and profile endpoints that are connected to the network devices.

- You must define Cisco TrustSec-enabled devices in Cisco ISE to process requests from TrustSec-enabled devices that can be part of the Cisco TrustSec solution. Any switch that supports the Cisco TrustSec solution is a Cisco TrustSec-enabled device.

  Cisco TrustSec devices do not use IP addresses. Instead, you must define other settings so that Cisco TrustSec devices can communicate with Cisco ISE.

  Cisco TrustSec-enabled devices use the TrustSec attributes to communicate with Cisco ISE. Cisco TrustSec-enabled devices, such as the Cisco Nexus 7000 Series Switches, Cisco Catalyst 6000 Series Switches, Cisco Catalyst 4000 Series Switches, and Cisco Catalyst 3000 Series Switches are authenticated using the Cisco TrustSec attributes that you define while adding Cisco TrustSec devices.

Note When you configure a network device on Cisco ISE, we recommend that you do not include a backslash (\) as part of the shared secret. This is because when you upgrade Cisco ISE, the backslash will not appear in the shared secret. However, if you reimage Cisco ISE instead of upgrading it, the backslash appears in the shared secret.

Define a Default Network Device in Cisco ISE

Cisco ISE supports the default device definition for RADIUS and TACACS authentications. You can define a default network device that Cisco ISE can use if it does not find a device definition for a particular IP address. This feature enables you to define a default RADIUS or TACACS shared secret and the level of access for newly provisioned devices.

Note We recommend that you add the default device definition only for basic RADIUS and TACACS authentications. For advanced flows, you must add a separate device definition for each network device.

Cisco ISE looks for the corresponding device definition to retrieve the shared secret that is configured in the network device definition when it receives a RADIUS or TACACS request from a network device.

Cisco ISE performs the following procedure when a RADIUS or TACACS request is received:

1. Looks for a specific IP address that matches the one in the request.

2. Looks up the ranges to see if the IP address in the request falls within the range that is specified.

3. If both step 1 and 2 fail, it uses the default device definition (if defined) to process the request.

Cisco ISE obtains the shared secret that is configured in the device definition for that device and matches it against the shared secret in the RADIUS or TACACS request to authenticate access. If no device definitions are found, Cisco ISE obtains the shared secret from the default network device definition and processes the RADIUS or TACACS request.

Network Devices

The windows described in the following sections enable you to add and manage network devices in Cisco ISE.

Network Device Definition Settings

The following tables describe the fields in the **Network Devices** window, which you can use to configure a network access device in Cisco ISE. To view this window, click the **Menu** icon (≡) and choose **Administration** > **Network Resources** > **Network Devices**, and click **Add**.

Network Device Settings

The following table describes the fields in the **New Network Devices** window.

Table 1: Network Device Settings

Field Name	Description
Name	Enter a name for the network device. You can provide a descriptive name to the network device, which is different from the hostname of the device. The device name is a logical identifier. **Note** If needed, the name of a device can be changed after it is configured.
Description	Enter a description for the device.

Field Name	Description
IP Address or **IP Range**	Choose one of the following from the drop-down list and enter the required values in the fields displayed: • **IP Address**: Enter a single IP address (IPv4 or IPv6 address) and a subnet mask. • **IP Range**: Enter the required IPv4 address range. To exclude IP addresses during authentication, enter an IP address or IP address range in the **Exclude** field. The following are the guidelines for defining the IP addresses and subnet masks, or IP address ranges: • You can define a specific IP address, or an IP range with a subnet mask. If device A has an IP address range defined, you can configure another device, B, with an individual address from the range that is defined in device A. • You can define IP address ranges in all the octets. You can use a hyphen (-) or an asterisk (*) as wildcard to specify a range of IP addresses. For example, *.*.*.*, 1-10.1-10.1-10.1-10, or 10-11.*.5.10-15. • You can exclude a subset of IP address range from the configured range in a scenario where that subset has already been added, for example, 10.197.65.*/10.197.65.1, or 10.197.65.* exclude 10.197.65.1. • You can configure up to 40 IP addresses or IP ranges for each network device. • You cannot define two devices with the same specific IP addresses. • You cannot define two devices with the same IP range. The IP ranges must not overlap either partially or completely. • When you exclude IP addresses, do not use overlapping IP ranges. Instead, exclude separate IP ranges.
Device Profile	Choose the vendor of the network device from the drop-down list. Use the tooltip next to the drop-down list to see the flows and services that the selected vendor's network devices support. The tooltip also displays the RADIUS Change of Authorization (CoA) port and type of URL redirect that is used by the device. These attributes are defined in the device type's network device profile.
Model Name	Choose the device model from the drop-down list. Use the model name as one of the parameters while checking for conditions in rule-based policies. This attribute is present in the device dictionary.
Software Version	Choose the version of the software running on the network device from the drop-down list. You can use the software version as one of the parameters while checking for conditions in rule-based policies. This attribute is present in the device dictionary.

Field Name	Description
Network Device Group	In the **Network Device Group** area, choose the required values from the **Location**, **IPsec**, and **Device Type** drop-down lists.
	If you do not specifically assign a device to a group, it becomes a part of the default device groups (root network device groups), which is **All Locations** by location and **All Device Types** by device type.

Note While using a filter to choose and delete a Network Access Device (NAD) from your Cisco ISE deployment, clear your browser cache to ensure that only chosen NADs are deleted.

RADIUS Authentication Settings

The following table describes the fields in the **RADIUS Authentication Settings** area.

Table 2: Fields in the RADIUS Authentication Settings Area

Field Name	Usage Guidelines
RADIUS UDP Settings	
Protocol	Displays **RADIUS** as the selected protocol.
Shared Secret	Enter the shared secret for the network device.
	The shared secret is the key that is configured on the network device using the **radius-host** command with the **pac** option.
	Note The length of the shared secret must be equal to or greater than the value configured in the **Minimum RADIUS Shared Secret Length** field in the **Device Security Settings** window (**Administration > Network Resources > Network Devices > Device Security Settings**).
	For a RADIUS server, the best practice is to have 22 characters. For new installations and upgraded deployments, the shared secret length is four characters by default. You can change this value in the **Device Security Settings** window.

Field Name	Usage Guidelines
Use Second Shared Secret	Specify a second shared secret to be used by the network device and Cisco ISE. **Note** Although Cisco TrustSec devices can take advantage of the dual shared secrets (keys), Cisco TrustSec CoA packets sent by Cisco ISE will always use the first shared secret (key). To enable the use of the second shared secret, choose the Cisco ISE node from which the Cisco TrustSec CoA packets must be sent to the Cisco TrustSec device. Configure the Cisco ISE node to be used for this task in the **Send From** drop-down list in the **Work Centers** > **Device Administration** > **Network Resources** > **Network Devices** > **Add** > **Advanced TrustSec Settings** window. You can select a primary administration node (PAN) or a policy service node (PSN). If the chosen PSN node is down, the PAN sends the Cisco TrustSec CoA packets to the Cisco TrustSec device. **Note** The Second Shared Secret feature for RADIUS Access Request works only for packets containing the **Message-Authenticator** field.
CoA Port	Specify the port to be used for RADIUS CoA. The default CoA port for the device is defined in the network device profile that is configured for a network device (**Administration** > **Network Resources** > **Network Device Profiles** > **Network Resources** > **Network Device Profiles**). Click **Set To Default** to use the default CoA port. **Note** If you modify the CoA port specified in the **Network Devices** window (**Administration** > **Network Resources** > **Network Devices**) under **RADIUS Authentication Settings**, make sure that you specify the same CoA port for the corresponding profile in the **Network Device Profile** window (**Administration** > **Network Resources** > **Network Device Profiles**).
RADIUS DTLS Settings	
DTLS Required	If you check the **DTLS Required** check box, Cisco ISE processes only the DTLS requests from this device. If this option is disabled, Cisco ISE processes both UDP and DTLS requests from this device. RADIUS DTLS provides improved security for Secure Sockets Layer (SSL) tunnel establishment and RADIUS communication.
Shared Secret	Displays the shared secret that is used for RADIUS DTLS. This value is fixed and used to compute the Message Digest 5 (MD5) integrity checks.
CoA Port	Specify the port to be used for RADIUS DTLS CoA.
Issuer CA of ISE Certificates for CoA	Choose the Certificate Authority to be used for RADIUS DTLS CoA from the drop-down list.
DNS Name	Enter the DNS name of the network device. If the **Enable RADIUS/DTLS Client Identity Verification** option is enabled in the **RADIUS Settings** window (**Adminstration** > **System** > **Settings** > **Protocols** > **RADIUS**, Cisco ISE compares this DNS name with the DNS name that is specified in the client certificate to verify the identity of the network device.

Field Name	Usage Guidelines
General Settings	
Enable KeyWrap	Check the **Enable KeyWrap** check box only if KeyWrap algorithms are supported by the network device. The network device must be compatible with AES KeyWrap RFC (RFC 3394). This option is used to increase the RADIUS security through an AES KeyWrap algorithm.
Key Encryption Key	Enter the encryption key that is used for session encryption (secrecy).
Message Authenticator Code Key	Enter the key that is used for keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages.
Key Input Format	Click one of the following radio buttons: • **ASCII**: The value that is entered in the **Key Encryption Key** field must be 16 characters (bytes) in length, and the value that is entered in the **Message Authenticator Code Key** field must be 20 characters (bytes) in length. • **Hexadecimal**: The value that is entered in the **Key Encryption Key** field must be 32 characters (bytes) in length, and the value that is entered in the **Message Authenticator Code Key** field must be 40 characters (bytes) in length. You can specify the key input format that you want to use to enter the Key Encryption Key and Message Authenticator Code Key so that it matches the configuration on the network device. The value that you specify must be the correct (full) length for the key, and shorter values are not permitted.

TACACS Authentication Settings

Table 3: Fields in the TACACS Authentication Settings Area

Field Name	Usage Guidelines
Shared Secret	A string of text that is assigned to a network device when TACACS+ protocol is enabled. The user must enter the text before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
Retired Shared Secret is Active	Displayed when the retirement period is active.
Retire	Retires an existing shared secret instead of ending it. When you click **Retire**, a dialog box is displayed. You can click either **Yes** or **No**.

Field Name	Usage Guidelines
Remaining Retired Period	(Available only if you click **Yes** in the **Retire** dialog box) Displays the default value that is specified in **Work Centers** > **Device Administration** > **Settings** > **Connection Settings** > **Default Shared Secret Retirement Period.** You can change the default value, as necessary. The old shared secret remains active for the specified number of days.
End	(Available only if you click **Yes** in the **Retire** dialog box) Ends the retirement period and terminates the old shared secret.
Enable Single Connect Mode	Check the **Enable Single Connect Mode** check box to use a single TCP connection for all TACACS communications with the network device. Click one of the following radio buttons: • **Legacy Cisco Devices** • **TACACS Draft Compliance Single Connect Support** **Note** If you disable **Single Connect Mode**, Cisco ISE uses a new TCP connection for every TACACS request.

SNMP Settings

The following table describes the fields in the **SNMP Settings** section.

Table 4: Fields in the SNMP Settings Area

Field Name	Usage Guidelines
SNMP Version	Choose one of the following options from the **SNMP Version** drop-down list: • **1**: SNMPv1 does not support informs. • **2c** • **3**: SNMPv3 is the most secure model because it allows packet encryption when you choose **Priv** in the **Security Level** field. **Note** If you have configured your network device with SNMPv3 parameters, you cannot generate the **Network Device Session Status** summary report that is provided by the monitoring service (**Operations** > **Reports** > **Diagnostics** > **Network Device Session Status**). You can generate this report successfully if your network device is configured with SNMPv1 or SNMPv2c parameters.
SNMP RO Community	(Applicable only for SNMP versions 1 and 2c) Enter the Read Only Community string that provides Cisco ISE with a particular type of access to the device. **Note** The caret (circumflex ^) symbol is not allowed.
SNMP Username	(Only for SNMP Version 3) Enter the SNMP username.

Field Name	Usage Guidelines
Security Level	(Only for SNMP Version 3) Choose one the following options from the **Security Level** drop-down list: • **Auth**: Enables MD5 or Secure Hash Algorithm (SHA) packet authentication. • **No Auth**: No authentication and no privacy security level. • **Priv**: Enables Data Encryption Standard (DES) packet encryption.
Auth Protocol	(Only for SNMP Version 3 when the security levels **Auth** or **Priv** are selected) Choose the authentication protocol that you want the network device to use from the **Auth Protocol** drop-down list. • **MD5** • **SHA**
Auth Password	(Only for SNMP Version 3 when the **Auth** or **Priv** security levels are selected) Enter the authentication key. It must be at least eight characters in length. Click **Show** to display the authentication password that is already configured for the device. **Note** The caret (circumflex ^) symbol cannot be used.
Privacy Protocol	(Only for SNMP Version 3 when **Priv** security level is selected) Choose one of the following options from the **Privacy Protocol** drop-down list: • **DES** • **AES128** • **AES192** • **AES256** • **3DES**
Privacy Password	(Only for SNMP Version 3 when **Priv** security level is selected) Enter the privacy key. Click **Show** to display the privacy password that is already configured for the device. **Note** The caret (circumflex ^) symbol cannot be used.
Polling Interval	Enter the polling interval, in seconds. The default value is 3600.
Link Trap Query	Check the **Link Trap Query** check box to receive and interpret linkup and linkdown notifications that are received through the SNMP trap.
Mac Trap Query	Check the **Link Trap Query** check box to receive and interpret MAC notifications received through the SNMP trap.

Field Name	Usage Guidelines
Originating Policy Services Node	Choose the Cisco ISE server to be used to poll for SNMP data, from the **Originating Policy Services Node** drop-down list. The default value for this field is **Auto**. Overwrite the setting by choosing a specific value from the drop-down list.

Advanced TrustSec Settings

The following table describes the fields in the **Advanced TrustSec Settings** section.

Table 5: Fields in the Advanced TrustSec Settings Area

Field Name	Usage Guidelines
Device Authentication Settings	
Use Device ID for TrustSec Identification	Check the **Use Device ID for TrustSec Identification** check box if you want the device name to be listed as the device identifier in the **Device ID** field.
Device ID	You can use this field only if you have not checked the **Use Device ID for TrustSec Identification** check box.
Password	Enter the password that you have configured in the Cisco TrustSec device's CLI to authenticate the Cisco TrustSec device. Click **Show** to display the password.
HTTP REST API Settings	
Enable HTTP REST API	Check the **Enable HTTP REST API** check box to use the HTTP REST API to provide the required Cisco TrustSec information to the network devices. This enhances the efficiency and ability to download large configurations in a short time as compared to the RADIUS protocol. It also improves reliability by using TCP over UDP.
Username	Enter the username that you have configured in the Cisco TrustSec device's CLI to authenticate the Cisco TrustSec device. The username cannot contain special characters such as space ! % ^ : ; , [{	}] ` ' " = < > ?
Password	Enter the password that you have configured in the Cisco TrustSec device's CLI to authenticate the Cisco TrustSec device.
TrustSec Device Notification and Updates	
Device ID	You can use this field only if you have not checked the **Use Device ID for TrustSec Identification** check box.
Password	Enter the password that you have configured in the Cisco TrustSec device's CLI to authenticate the Cisco TrustSec device. Click **Show** to display the password.

Field Name	Usage Guidelines
Download Environment Data Every <...>	Specify the time interval at which the device must download its environment data from Cisco ISE, by choosing the required values from the drop-down lists in this area. You can choose the time interval in seconds, minutes, hours, days, or weeks. The default value is one day.
Download Peer Authorization Policy Every <...>	Specify the time interval at which the device must download the peer authorization policy from Cisco ISE by choosing the required values from the drop-down lists in this area. You can specify the time interval in seconds, minutes, hours, days, or weeks. The default value is one day.
Reauthentication Every <...>	Specify the time interval at which the device reauthenticates itself against Cisco ISE after the initial authentication, by choosing the required values from the drop-down lists in this area. You can configure the time interval in seconds, minutes, hours, days, or weeks. For example, if you enter 1000 seconds, the device authenticates itself against Cisco ISE every 1000 seconds. The default value is one day.
Download SGACL Lists Every <...>	Specify the time interval at which the device downloads SGACL lists from Cisco ISE, by choosing the required values from the drop-down lists in this area. You can configure the time interval in seconds, minutes, hours, days, or weeks. The default value is one day.
Other TrustSec Devices to Trust This Device (TrustSec Trusted)	Check the **Other TrustSec Devices to Trust This Device** check box to allow all the peer devices to trust this Cisco TrustSec device. If this check box is not checked, the peer devices do not trust this device, and all the packets that arrive from this device are colored or tagged accordingly.
Send Configuration Changes to Device	Check the **Send Configuration Changes to Device** check box if you want Cisco ISE to send Cisco TrustSec configuration changes to the Cisco TrustSec device using CoA or CLI (SSH). Click the **CoA** or **CLI (SSH)** radio button, as required.
	Click the **CoA** radio button if you want Cisco ISE to send the configuration changes to the Cisco TrustSec device using CoA.
	Click the **CLI (SSH)** radio button if you want Cisco ISE to send the configuration changes to the Cisco TrustSec device using the CLI (using the SSH connection). For more information, see Push Configuration Changes to Non-CoA Supporting Devices.
Send From	From the drop-down list, choose the Cisco ISE node from which the configuration changes must be sent to the Cisco TrustSec device. You can select a PAN or a PSN. If the PSN that you choose is down, the configuration changes are sent to the Cisco TrustSec device using the PAN.
Test Connection	You can use this option to test the connectivity between the Cisco TrustSec device and the selected Cisco ISE node (PAN or PSN).
SSH Key	To use this feature, open an SSHv2 tunnel from Cisco ISE to the network device, and use the device's CLI to retrieve the SSH key. You must copy this key and paste it in the **SSH Key** field for validation. For more information, see SSH Key Validation.
Device Configuration Deployment	

Field Name	Usage Guidelines
Include this device when deploying Security Group Tag Mapping Updates	Check the **Include this device when deploying Security Group Tag Mapping Updates** check box if you want the Cisco TrustSec device to obtain the IP-SGT mappings using the device interface credentials.
EXEC Mode Username	Enter the username that you use to log in to the Cisco TrustSec device.
EXEC Mode Password	Enter the device password. Click **Show** to view the password. **Note** We recommend that you avoid using the % character in passwords, including in the EXEC modes and Enable mode passwords to avoid security vulnerabilities.
Enable Mode Password	(Optional) Enter the enable password that is used to edit the configuration of the Cisco TrustSec device in privileged EXEC mode. Click **Show** to view the password.
Out Of Band TrustSec PAC	
Issue Date	Displays the issuing date of the last Cisco TrustSec PAC that was generated by Cisco ISE for the Cisco TrustSec device.
Expiration Date	Displays the expiration date of the last Cisco TrustSec PAC that was generated by Cisco ISE for the Cisco TrustSec device.
Issued By	Displays the name of the issuer (a Cisco TrustSec administrator) of the last Cisco TrustSec PAC that was generated by Cisco ISE for the Cisco TrustSec device.
Generate PAC	Click the **Generate PAC** button to generate the out-of-band Cisco TrustSec PAC for the Cisco TrustSec device.

Default Network Device Definition Settings

The following table describes the fields in the **Default Network Device** window, with which you configure a default network device that Cisco ISE can use for RADIUS or TACACS+ authentication. Choose one of the following navigation paths:

- **Administration** > **Network Resources** > **Network Devices** > **Default Device**

- **Work Centers** > **Device Administration** > **Network Resources** > **Default Devices**

Table 6: Fields in the Default Network Device Window

Field Name	Usage Guidelines
Default Network Device Status	Choose **Enable** from the **Default Network Device Status** drop-down list to enable the default network device definition. **Note** If the default device is enabled, you must enable either the RADIUS or the TACACS+ authentication settings by checking the relevant check box in the window.
Device Profile	Displays **Cisco** as the default device vendor.
RADIUS Authentication Settings	
Enable RADIUS	Check the **Enable RADIUS** check box to enable RADIUS authentication for the device.
RADIUS UDP Settings	
Shared Secret	Enter a shared secret. The shared secret can be up to 127 characters in length. The shared secret is the key that you have configured on the network device using the **radius-host** command with the **pac** keyword. **Note** The length of the shared secret must be equal to or greater than the value configured in the **Minimum RADIUS Shared Secret Length** field in the **Device Security Settings** window (**Administration** > **Network Resources** > **Network Devices** > **Device Security Settings**). By default, this value is four characters for new installations and upgraded deployments. For the RADIUS server, the best practice is to have 22 characters.
RADIUS DTLS Settings	
DTLS Required	If you check the **DTLS Required** check box, Cisco ISE processes only the DTLS requests from this device. If this option is disabled, Cisco ISE processes both UDP and DTLS requests from this device. RADIUS DTLS provides improved security for SSL tunnel establishment and RADIUS communication.
Shared Secret	Displays the shared secret that is used for RADIUS DTLS. This value is fixed and is used to compute the MD5 integrity checks.
Issuer CA of ISE Certificates for CoA	Choose the certificate authority to be used for RADIUS DTLS CoA from the **Issuer CA of ISE Certificates for CoA** drop-down list.
General Settings	
Enable KeyWrap	(Optional) Check the **Enable KeyWrap** check box only if KeyWrap algorithms are supported on the network device, which increases RADIUS security through an AES KeyWrap algorithm.

Field Name	Usage Guidelines
Key Encryption Key	Enter an encryption key to be used for session encryption (secrecy) when you enable KeyWrap.
Message Authenticator Code Key	Enter the key that is used for keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages when you enable KeyWrap.
Key Input Format	Choose one of the following formats by clicking the corresponding radio button, and enter values in the **Key Encryption Key** and **Message Authenticator Code Key** fields: • **ASCII**: The **Key Encryption Key** must be 16 characters (bytes) in length, and the **Message Authenticator Code Key** must be 20 characters (bytes) in length. • **Hexadecimal**: The **Key Encryption Key** must be 32 bytes in length, and the **Message Authenticator Code Key** must be 40 bytes in length. Specify the key input format that you want to use to enter the Key Encryption Key and Message Authenticator Code Key so that it matches the configuration on the network device. The value that you specify must be the correct (full) length for the key. Shorter values are not permitted.
TACACS Authentication Settings	
Shared Secret	Enter a string of text to assign to a network device when the TACACS+ protocol is enabled. Note that a user must enter the text before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
Retired Shared Secret is Active	Displayed when the retirement period is active.
Retire	Retires an existing shared secret instead of ending it. When you click **Retire**, a dialog box is displayed. Click **Yes** or **No**.
Remaining Retired Period	(Optional) Available only if you click **Yes** in the **Retire** dialog box. Displays the default value that is specified in the **Work Centers** > **Device Administration** > **Settings** > **Connection Settings** > **Default Shared Secret Retirement Period** window. You can change the default values. This allows a new shared secret to be entered. The old shared secret remains active for the specified number of days.
End	(Optional) Available only if you select **Yes** in the **Remaining Retired Period** dialog box. Ends the retirement period and terminates the old shared secret.

Field Name	Usage Guidelines
Enable Single Connect Mode	Check the **Enable Single Connect Mode** check box to use a single TCP connection for all TACACS+ communication with the network device. Click one of the following the radio buttons: • **Legacy Cisco Devices** • **TACACS Draft Compliance Single Connect Support**. **Note** If you disable this field, Cisco ISE uses a new TCP connection for every TACACS+ request.

Network Device Import Settings

The following table describes the fields in the **Import Network Devices** window, which you can use to import network device details into Cisco ISE. To view this window, click the **Menu** icon (≡) and choose **Administration** > **Network Resources** > **Network Devices**. In the **Network Devices** window, click **Import**.

Table 7: Import Network Devices Settings

Field Name	Usage Guidelines
Generate a Template	Click **Generate a Template** to create a comma-separated value (CSV) template file. Update the template with network devices information in the CSV format and save it locally. Then, use the edited template to import network devices into any Cisco ISE deployment.
File	Click **Choose File** to choose the CSV file that you have recently created, or previously exported from a Cisco ISE deployment. You can import network devices into another Cisco ISE deployment with new and updated network devices information, by using the **Import** option.
Overwrite Existing Data with New Data	Check the **Overwrite Existing Data with New Data** check box to replace the existing network devices with the devices in your import file. If you do not check this check box, new network device definitions that are available in the import file are added to the network device repository. Duplicate entries are ignored.
Stop Import on First Error	Check the **Stop Import on First Error** check box if you want Cisco ISE to discontinue import when it encounters an error during import. Cisco ISE imports network devices until the time of an error. If this check box is not checked and an error is encountered, the error is reported and Cisco ISE continues to import the remaining devices.

Add a Network Device in Cisco ISE

You can add a network device in Cisco ISE or use the default network device.

You can also add a network device in the **Network Devices** (**Work Centers** > **Device Administration** > **Network Resources** > **Network Devices**) window.

Before you begin

The AAA function must be enabled on the network device to be added. See Command to Enable AAA Functions.

Step 1	In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration** > **Network Resources** > **Network Devices**.
Step 2	Click **Add**.
Step 3	Enter the corresponding values in the **Name**, **Description**, and **IP Address** fields.
Step 4	Choose the required values from the **Device Profile**, **Model Name**, **Software Version**, and **Network Device Group** drop-down lists.
Step 5	(Optional) Check the **RADIUS Authentication Settings** check box to configure the RADIUS protocol for authentication.
Step 6	(Optional) Check the **TACACS Authentication Settings** check box to configure the TACACS protocol for authentication.
Step 7	(Optional) Check the **SNMP Settings** check box to configure SNMP for the Cisco ISE profiling service to collect information from the network device.
Step 8	(Optional) Check the **Advanced Trustsec Settings** check box to configure a Cisco TrustSec-enabled device.
Step 9	Click **Submit**.

Import Network Devices into Cisco ISE

To enable Cisco ISE to communicate with network devices, you must add device definitions of the network devices in Cisco ISE. Import device definitions of network devices into Cisco ISE through the **Network Devices** window (From the main menu, choose **Administration** > **Network Resources** > **Network Devices**).

Import a list of device definitions into a Cisco ISE node using a comma-separated value (CSV) file. A CSV template file is available when you click **Import** in the **Network Devices** window. Download this file, enter the required device definitions, and then upload the edited file through the **Import** window.

You cannot execute multiple imports of the same resource type at the same time. For example, you cannot concurrently import network devices from two different import files.

When you import a CSV file of device definitions, you can either create new records or update existing records by clicking the **Overwrite Existing Data with New Data** option.

Import templates may vary in each Cisco ISE. Do not import CSV files of network devices that have exported from a different Cisco ISE release. Enter the details of the network devices in the CSV template file for your release, and import this file into Cisco ISE.

Note You can import the network devices with IP ranges in all the octets.

Step 1	In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration** > **Network Resources** > **Network Devices**.
Step 2	Click **Import**.

Step 3   In the **Import Network Devices** window that is displayed, click **Generate A Template** to download a CSV file that you can edit and then import it into Cisco ISE with the required details.

Step 4   Click **Choose File** to choose the CSV file from the system that is running the client browser.

Step 5   (Optional) Check the for **Overwrite Existing Data with New Data** and **Stop Import on First Error**check boxes, as required.

Step 6   Click **Import**.

After the file import is complete, Cisco ISE displays a summary message. This message includes the import status (successful or unsuccessful), number of errors encountered, if any, and the total processing time taken for the file import process.

Export Network Devices from Cisco ISE

Export the device definitions of the network devices that are available in a Cisco ISE node in the form of a CSV file. You can then import this CSV file into another Cisco ISE node so that the device definitions are available to the required Cisco ISE nodes.

Note   You can export the network devices with IP ranges in all the octets.

Step 1   In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration** > **Network Resources** > **Network Devices**.

Step 2   Click **Export**.

Step 3   Export the device definitions for the network devices added to the Cisco ISE node by performing one of the following actions.

- Check the check boxes next to the devices that you want to export, choose **Export Selected** from the **Export** drop-down list.

- Choose **Export All** from the **Export** drop-down list to export all the network devices that are added to the Cisco ISE node.

Step 4   In both cases, a CSV file of device definitions downloads to your system.

Troubleshoot Network Device Configuration Issues

Step 1   In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **Evaluate Configuration Validator**.

Step 2   Enter the IP address of the network device that you want to evaluate in the **Network Device IP** field.

Step 3   Check the check boxes and click the radio buttons next to the configuration options you want to compare against the recommended template.

Step 4   Click **Run**.

Step 5   In the **Progress Details...** area, click **Click Here to Enter Credentials**.

Step 6 In the **Credentials Window** dialog box, enter the connection parameters and credentials that are required to establish a connection with the network devices.

Step 7 Click **Submit**.

Step 8 (Optional) To cancel the workflow, click **Click Here to Cancel the Running Workflow** in the **Progress Details...** window.

Step 9 (Optional) Check the check boxes next to the interfaces that you want to analyze, and click **Submit**.

Step 10 (Optional) Click **Show Results Summary** for details of the configuration evaluation.

The Execute Network Device Command Diagnostic Tool

The Execute Network Device Command diagnostic tool allows you to run the **show** command on any network device.

The results that are displayed are the same as what you would see on a console. The tool enables you to identify problems, if any, in a device configuration.

Use this tool to validate the configuration of any network device, or if you are want to know how a network device is configured.

To access the Execute Network Device Command diagnostic tool, choose one of the following navigation paths:

1. In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **Execute Network Device Command**.In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Work Centers** > **Profiler** > **Troubleshoot** > **Execute Network Device Command**.

2. In the **Execute Network Device Command** window that is displayed, enter the IP address of the network device and the **show** command that you want to run in the corresponding fields.

3. Click **Run**.

Third-Party Network Device Support in Cisco ISE

Cisco ISE supports third-party network access devices (NADs) by using network device profiles. A NAD profile defines the capabilities of a third-party device with a simplified policy configuration, regardless of the vendor-side implementation. A network device profile contains the following:

- The protocols that the network device supports, such as RADIUS, TACACS+, and Cisco TrustSec. You can import into Cisco ISE any vendor-specific RADIUS dictionaries that exist for the network device.

- The attributes and values that the device uses for various authentication flows such as Wired MAB and 802.1X. These attributes and values allow Cisco ISE to detect the right authentication flow for your device according to the attributes that the network device uses.

- The Change of Authorization (CoA) capabilities of the network device. While the RADIUS protocol RFC 5176 defines a CoA request, the attributes used in a CoA request vary depending on the network device. Most non-Cisco devices with RFC 5176 support the *Push* and *Disconnect* functions. For devices that do not support the RADIUS CoA type, Cisco ISE also supports SNMP CoA.

- The attributes and protocols that the network device uses for MAB flows. Network devices from different vendors perform MAB authentication differently.

- The VLAN and ACL permissions that are used by the device. When you save the profile, Cisco ISE automatically generates authorization profiles for each configured permission.

- URL redirection technique information. URL redirection is necessary for advanced flows such as Bring Your Own Device (BYOD), guest access, and posture services. Two types of URL redirections are found on a network device—static and dynamic. For static URL redirection, you can copy and paste the Cisco ISE portal URL into the configuration. For dynamic URL redirection, Cisco ISE uses a RADIUS attribute to tell the network device where to redirect to.

  If the network device does not support both dynamic and static URL redirects, Cisco ISE provides an Auth VLAN configuration by which URL redirect is simulated. The Auth VLAN configuration is based on DHCP and DNS services running in Cisco ISE.

After you have defined your network devices in Cisco ISE, configure these device profiles or use the preconfigured device profiles that are offered by Cisco ISE to define the capabilities that Cisco ISE uses to enable basic authentication flows, and advanced flows such as Profiler, Guest, BYOD, MAB, and Posture.

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

The following is an example of an Auth VLAN flow:

1. A guest endpoint connects to the NAD.

2. The network device sends the RADIUS or MAB request to Cisco ISE.

3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.

4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.

5. The guest endpoint receives network access.

6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.

7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.

8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.

9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.

10. The guest endpoint user logs in for authentication.

11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.

12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN.

Multiple VLANs may be connected to one network interface card by configuring a VLAN IP helper from the NAD configuration. For more information about configuring an IP helper, see the administration guide for the network device for instructions. For guest access flows that include VLANs with IP helpers, define a guest portal, and select that portal in an authorization profile that is bound to MAB authorization. For more information about guest portals, see Cisco ISE Guest Services.
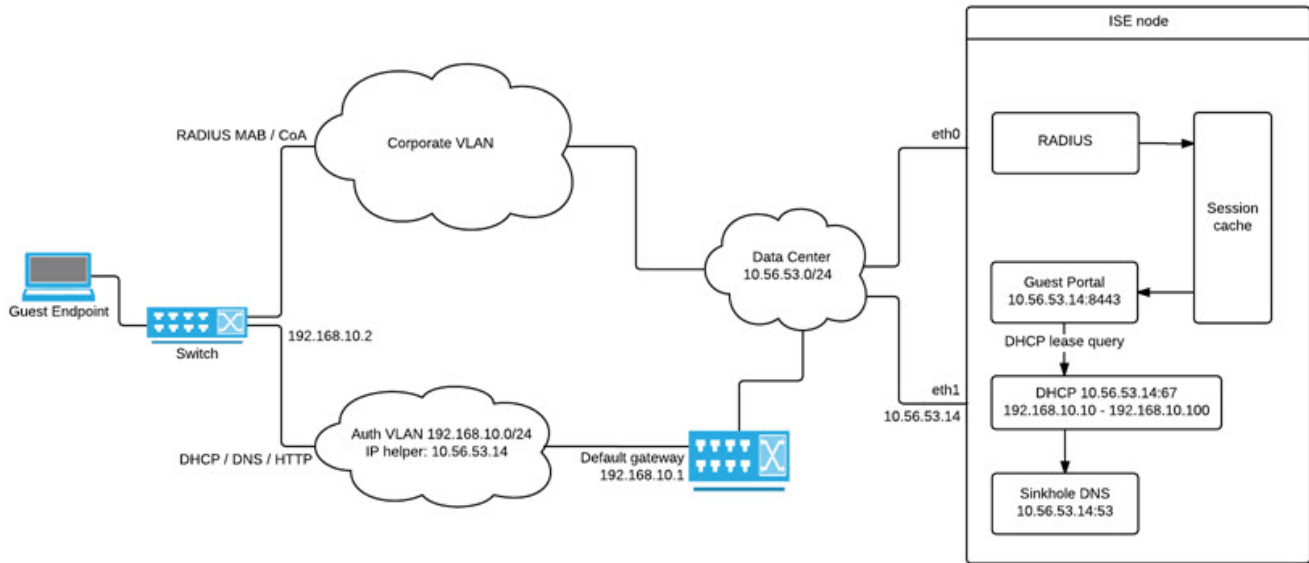
The following diagram displays a basic network setup when an Auth VLAN is defined (the Auth VLAN is connected directly to a Cisco ISE node).

Figure 1: Auth VLAN Connected to Cisco ISE Node
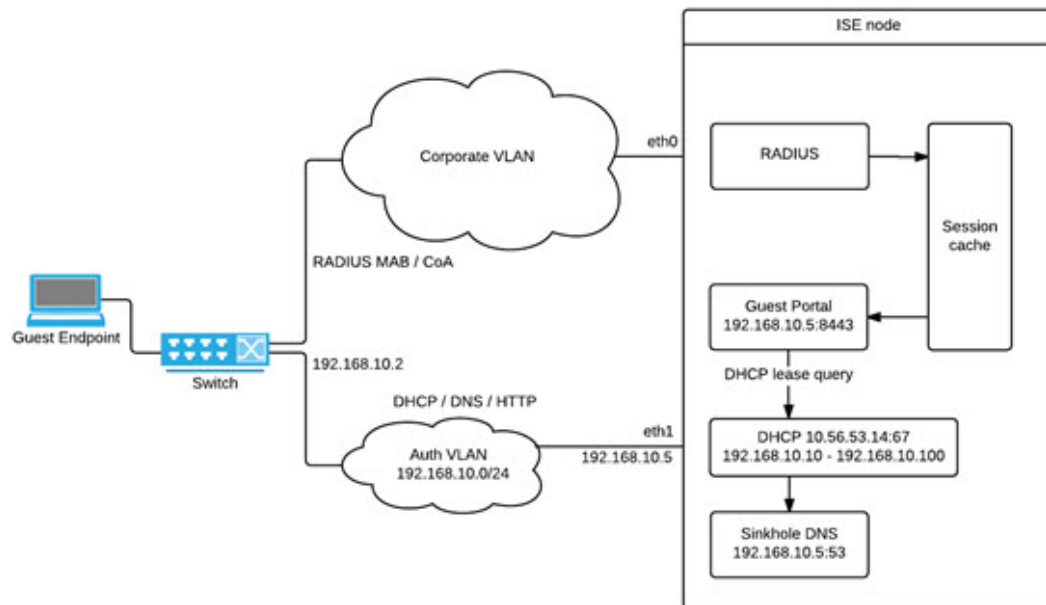
The following diagram displays a network with Auth VLAN and an IP helper.

Figure 2: Auth VLAN Configured with IP Helper

CoA Types

Cisco ISE supports both RADIUS and SNMP CoA types. RADIUS or SNMP CoA type support is required for the NAD to work in complex flows, while it is not mandatory for basic flows.

Define the RADIUS and SNMP settings that the network device supports when you configure the NAD in Cisco ISE. Indicate the CoA type to be used for a specific flow when configuring the NAD profile. For more information about defining protocols for your NADs, see Network Device Definition Settings, on page 3. Check with your third-party supplier to verify which CoA type your NAD supports before creating the device profile and NAD profile in Cisco ISE.

Network Device Profiles

Cisco ISE supports some third-party NADs by using network device profiles. These profiles define the capabilities that Cisco ISE uses to enable basic flows, and advanced flows such as Guest, BYOD, MAB, and Posture.

Cisco ISE includes predefined profiles for network devices from several vendors. Cisco ISE 2.1 and later releases have been tested with the network devices listed in the following table.

Table 8: Vendor Devices Tested with Cisco ISE 2.1 and Later Releases

Device Type	Vendor	CoA Type	URL Redirect Type	Supported or Validated Use Cases				
				802.1X and MAB Flows	Profiler without CoA	Profiler with CoA	Posture	Guest and BYOD Flows

Wireless	Aruba 7000, InstantAP	RADIUS	Static URL	Yes	Yes	Yes	Yes	Yes
	Motorola RFS 4000	RADIUS	Dynamic URL	Yes	Yes	Yes	Yes	Yes
	HP 830	RADIUS	Static URL	Yes	Yes	Yes	Yes	Yes
	Ruckus ZD 1200	RADIUS	—	Yes	Yes	Yes	Yes	Yes
Wired	HP A5500	RADIUS	Auth VLAN provided by ISE	Yes	Yes	Yes	Yes	Yes
	HP 3800 and 2920 (ProCurve)	RADIUS	Auth VLAN provided by ISE	Yes	Yes	Yes	Yes	Yes
	Alcatel 6850	SNMP	Dynamic URL	Yes	Yes	Yes	Yes	Yes
	Brocade ICX 6610	RADIUS	Auth VLAN provided by ISE	Yes	Yes	Yes	Yes	Yes
	Juniper EX3300-24p	RADIUS	Auth VLAN provided by ISE	Yes	Yes	Yes	Yes	Yes
For other third-party NADs, you must identify the device properties and capabilities, and create custom NAD profiles in Cisco ISE.				Yes	Yes	Requires CoA support	Requires CoA support. If a wired device does not support URL redirect, Cisco ISE uses Auth VLAN. Wireless devices have not been tested with Auth VLAN.	

You must create custom NAD profiles for other third-party network devices that do not have a predefined profile. For advanced workflows such as Guest, BYOD, and Posture, the network device must support the RADIUS protocol RFC 5176, which pertains to CoA support for these flows. See the device's administration guide for information on the attributes that are required to create network device profiles in Cisco ISE.

ISE Community Resource

For information about third-party NAD profiles, see ISE Third-Party NAD Profiles and Configs.

Configure a Third-Party Network Device in Cisco ISE

Cisco ISE supports third-party NADs by using network device profiles. These profiles define the capabilities that Cisco ISE uses to enable flows such as Guest, BYOD, MAB, and Posture.

Before you begin

See Network Device Profiles, on page 21.

Step 1 Add the third-party network device to Cisco ISE (See Import Network Devices into Cisco ISE, on page 16. If you are configuring Guest, BYOD, or Posture workflows, ensure that CoA is defined and the NAD's URL redirect mechanism is configured to point to the relevant Cisco ISE portal. To configure the URL redirect, copy the Cisco ISE portal URL from the portal's landing page. For more information about configuring CoA types and URL redirects for the NAD in Cisco ISE, see Network Device Definition Settings, on page 3. In addition, see the third-party device's administration guide for instructions.

Step 2 Ensure that an appropriate NAD profile for your device is available in Cisco ISE. To view the existing profiles, choose **Administration** > **Network Resources** > **Network Device Profiles**. If an appropriate profile does not exist in Cisco ISE, create a custom profile. See Create a Network Device Profile, on page 23 for information on how to create custom profiles.

Step 3 Assign a NAD profile to the NAD that you want to configure. In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration** > **Network Resources** > **Network Devices**. Open the device to which you want to assign a profile, and from the **Device Profile** drop-down list, choose the profile that you want to assign.

Step 4 When you configure your policy rules, set the authorization profile to the NAD profile in step 1, or **Any** if you are just using VLAN or ACL, or if you have different devices from different vendors in your network. To set the NAD profile for the authorization profile, choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**. Open the relevant authorization profile and from the **Network Device Profile** drop-down list, choose the relevant NAD profile. When using Auth VLAN for Guest flows, you should also define a guest portal and select that portal in an Authorization profile that is bound to MAB authorization—similar to regular Guest flows. For more information about guest portals, see the "Cisco ISE Guest Services" section in see Cisco ISE Guest Services.

Create a Network Device Profile

Before you begin

- Most NADs have a vendor-specific RADIUS dictionary that provides several vendor-specific attributes, apart from the standard IETF RADIUS attributes. If the network device has a vendor-specific RADIUS dictionary, import it into Cisco ISE. See the third-party device's administration guide for instructions on which RADIUS dictionary is required. In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Policy** > **Policy Elements** > **Dictionaries** > **System** > **Radius** > **RADIUS Vendors**. To import RADIUS dictionaries, see Create RADIUS-Vendor Dictionaries.

- For complex flows such as Guest and Posture, the network device must support the CoA types that are defined in RFC 5176

- For information about the fields and possible values for creating a network device profile, see Network Device Profiles Settings.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration** > **Network Resources** > **Network Device Profiles**.

Step 2 Click **Add**.

Step 3   In the **New Network Device Profile** window that is displayed, enter the corresponding values in the **Name** and **Description** fields for the network device.

Step 4   From the **Vendor** drop-down list, choose the vendor of the network device.

Step 5   In the **Icon** area, click **Change Icon...** to upload an icon for the network device from your system.

Alternatively, in the **Icon** area, click **Set To Default** to use the default icon provided by Cisco ISE.

Step 6   In the **Supported Protocols** area, check the check boxes for the protocols that the device supports. Check the check boxes only for the protocols that you want to actually use. If the network device supports the RADIUS protocol, choose the RADIUS dictionary to be used in the device from **RADIUS Dictionaries** drop-down list.

Step 7   In the **Templates** area, enter relevant details:

   a) Click **Authentication/Authorization** to configure the network device's default settings for flow types, attribute aliasing, and host lookup. In the new **Flow Type Conditions** area that is displayed, enter the attributes and values that your device uses for various authentication and authorization flows such as Wired MAB or 802.1X. This enables Cisco ISE to detect the correct flow type for your device according to the attributes it uses. There is no IETF standard for MAB, and different vendors use different values for Service Type. See the device's user guide or use a sniffer trace of a MAB authentication to determine the correct settings. In the **Attribute Aliasing** area, map device-specific attribute names to common names to simplify policy rules. Currently, only the Service Set Identifier (SSID) is defined. If the network device has the concept of wireless SSID, then set this to the attribute it uses. Cisco ISE maps this to an attribute called SSID in the Normalized RADIUS dictionary. This simplifies policy rule configuration because you can refer to SSID in one rule, and it works for multiple devices even if the underlying attributes are different. In the **Host Lookup** area, check the **Process Host Lookup** check box and select the relevant MAB protocols and attributes for your device, based on the instructions provided by the third-party device vendor.

   b) Click **Permissions** to configure the network device's default settings for VLAN and ACL. These are automatically mapped based on the authorization profiles that you create in Cisco ISE.

   c) Click **Change of Authorization (CoA)** to configure the network device's CoA capabilities.

   If you choose **RADIUS** from the **CoA By** drop-down list, in the configurations area that is displayed, you must choose only static attributes. Dynamic attributes are not supported.

   d) Click **Redirect** to configure the network device's URL-redirect capabilities. URL redirection is necessary for guest, BYOD, and posture services.

Step 8   Click **Submit**.

> **Related Topics**
> How to Create ISE Network Access Device Profiles

Export Network Device Profiles from Cisco ISE

Export single or multiple network device profiles that are configured in Cisco ISE in the form of an XML file. The XML file can then be edited and imported into Cisco ISE file as new network profiles.

Before you begin

See How to Create ISE Network Access Device Profiles.

Step 1   In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration** > **Network Resources** > **Network Device Profiles**.

Step 2   Check the check boxes next to the devices that you want to export, and click **Export Selected**.

Step 3   A file that is named **DeviceProfiles.xml** downloads to your local hard disk.

Import Network Device Profiles into Cisco ISE

Import a single or multiple network device profiles into Cisco ISE using a single XML file with the Cisco ISE XML structure. You cannot concurrently import network device profiles from multiple import files.

Typically, you must first export an existing profile from the Cisco ISE administrator portal to use as a template. Enter your device profile details in the file, and save it as an XML file. Then, import the edited file back into Cisco ISE. To work with multiple network device profiles, export multiple profiles that are structured together as a single XML file, edit the file, and then import the profiles together to create multiple profiles in Cisco ISE.

When you import network device profiles, you can only create new records. You cannot overwrite an existing profile. To update an existing network device profile, export the existing profile from Cisco ISE, delete the profile from Cisco ISE, and then import the profile after you edit it accordingly.

Before you begin

See How to Create ISE Network Access Device Profiles.

Step 1   In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration** > **Network Resources** > **Network Device Profiles**.

Step 2   Click **Import**.

Step 3   Click **Choose File** to choose the XML file from the system that is running the client browser.

Step 4   Click **Import**.

Manage Network Device Groups

The following windows enable you to configure and manage network device groups.

Network Device Group Settings

The following table describes the fields in the **Network Device Groups** window that you use to create network device groups. To view this window, click the **Menu** icon (≡) and choose **Administration** > **Network Resources** > **Network Device Groups** > **All Groups**.

You can also create network device groups in the **Work Centers** > **Device Administration** > **Network Resources** > **Network Device Groups** > **All Groups** window.

Table 9: Fields in the Network Device Group Window

Field Name	Usage Guidelines
Name	Enter a name for the root network device group. For all subsequent child network device groups added to this root network device group, enter the name of this newly created network device group. You can have a maximum of six nodes in a network device group hierarchy, including the root node. Each network device group name can have a maximum of 32 characters.
Description	Enter a description for the root or the child network device group.
No. of Network Devices	The number of network devices in the network group is displayed in this column.

Network Device Group Import Settings

The following table describes the fields in the **Import** dialog box in the **Network Device Group** window. To view this window, click the **Menu** icon (≡) and choose **Administration** > **Network Resources** > **Network Device Groups**.

Table 10: Fields in the Network Device Groups Import Window

Field Name	Usage Guidelines
Generate a Template	Click this link to download a CSV template file. Update the template with network device group information in the same format. Save the template locally to import the network device groups into any Cisco ISE deployment.
File	Click **Choose File** and navigate to the location of the CSV file that you want to upload. The file may be new or a file that was exported from another Cisco ISE deployment. You can import network device groups from one Cisco ISE deployment to another, with new and updated network device groups information.
Overwrite Existing Data with New Data	Check this check box if you want to replace the existing network device groups with the device groups in your import file. If you do not check this check box, only the new network device groups in the import file are added to the network device group repository. Duplicate entries are ignored.
Stop Import on First Error	Check this check box to discontinue import at the first instance of encountering an error during the import. If this check box is not checked and an error is encountered, Cisco ISE reports the error and continues importing the rest of the device groups.

Network Device Groups

Cisco ISE allows you to create hierarchical network device groups. Use network device groups to logically group network devices based on various criteria, such as geographic location, device type, or its relative place in the network (such as Access Layer or Data Center).

To view the Network Device Groups window, click the **Menu** icon (≡) and choose **Administration** > **Network Resources** > **Network Device Groups**.

For example, to organize your network devices based on geographic location, group them by continent, region, or country:

- **Africa** > **Southern** > **Namibia**

- **Africa** > **Southern** > **South Africa**

- **Africa** > **Southern** > **Botswana**

Group the network devices based on the device type:

- **Africa** > **Southern** > **Botswana** > **Firewalls**

- **Africa** > **Southern** > **Botswana** > **Routers**

- **Africa** > **Southern** > **Botswana** > **Switches**

Assign network devices to one or more hierarchical network device groups. When Cisco ISE processes the ordered list of configured network device groups to determine the appropriate group to assign to a particular device, it may find that the same device profile applies to multiple device groups. In this case, Cisco ISE applies the first device group that is matched.

There is no limit on the maximum number of network device groups that you can create. You can create up to six levels of hierarchy (including the parent group) for the network device groups.

The device group hierarchy is displayed in two views, **Tree Table** and **Flat Table**. Click **Tree Table** or **Flat Table** above the list of network device groups to organize the list into the corresponding view.

In the **Tree Table** view, the root node appears at the top of the tree followed by the child groups in hierarchical order. Click **Expand All** to view all the device groups in each root group. Click **Collapse All** to view a list of only the root groups.

In the **Flat Table** view, the hierarchy of each device group is displayed in the **Group Hierarchy** column.

In both views, the number of network devices that are assigned to each child group is displayed in the corresponding **No. of Network Devices** column. Click the number to launch a dialog box that lists all the network devices that are assigned to that device group. The dialog box that is displayed also contains two buttons to move network devices from one group to another. Click **Move Devices to Another Group** to move network devices from the current group to another. Click **Add Devices to Group** to move a network device into the chosen network device group.

To add a network device group in the **Network Device Groups** window, click **Add**. In the **Parent Group** drop-down list, choose the parent group to which the network device group must be added, or choose the **Add As Root Group** option to add the new network device group as the parent group.

![note icon]

Note You cannot delete a device group if any devices are assigned to that device group. Before deleting a device group, you must move all the existing devices to another device group.

Root Network Device Groups

Cisco ISE includes two predefined root network device groups, **All Device Types** and **All Locations**. You cannot edit, duplicate, or delete these predefined network device groups, but you can add new device groups under them.

You can create a root Network Device Group (network device group), and then create child network device groups under the root group in the **Network Device Groups** window, as described earlier.

Network Device Attributes Used by Cisco ISE in Policy Evaluation

When you create a new network device group, a new network device attribute is added to the **Device** dictionary in **System Dictionaries** (**Policy** > **Policy Elements** > **Dictionaries**). The added device attributes are then used in policy definitions.

Cisco ISE allows you to configure authentication and authorization policies using **Device** dictionary attributes such as the device type, location, model name, or software version that is running on the network device.

Import Network Device Groups into Cisco ISE

You can import network device groups into a Cisco ISE node using a comma-separated value (CSV) file. Not that you cannot concurrently import network device groups from two different import files.

Download a CSV template from the Cisco ISE administrator portal. Enter your network device group details in the template, save the template as a CSV file, and then import the edited file into Cisco ISE.

When importing device groups, you can create new records or update existing records. When you import device groups, you can also define whether you want Cisco ISE to overwrite the existing device groups with the new groups or stop the import process when Cisco ISE encounters the first error.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration** > **Network Resources** > **Network Device Groups**.

Step 2 Click **Import**.

Step 3 In the dialog box, click **Choose File** to choose the CSV file from the system that is running the client browser.

To download a CSV template file for adding network device groups, click **Generate a Template**.

Step 4 To overwrite the existing network device groups, check the **Overwrite Existing Data with New Data** check box.

Step 5 Check the **Stop Import on First Error** check box.

Step 6 Click **Import**.

Export Network Device Groups from Cisco ISE

You can export network device groups that are configured in Cisco ISE in the form of a CSV file. You can then import these network device groups into another Cisco ISE node.

Step 1   In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration** > **Network Resources** > **Network Device Groups** > **All Groups**.

Step 2   To export the network device groups, you can do one of the following:

- Check the check boxes next to the device groups that you want to export, and choose **Export** > **Export Selected**.

- Choose **Export** > **Export All** to export all the network device groups that are defined.

A CSV file is downloaded into your local hard disk.

Manage Network Device Groups

The following windows enable you to configure and manage network device groups.

Network Device Group Settings

The following table describes the fields in the **Network Device Groups** window that you use to create network device groups. To view this window, click the **Menu** icon (≡) and choose **Administration** > **Network Resources** > **Network Device Groups** > **All Groups**.

You can also create network device groups in the **Work Centers** > **Device Administration** > **Network Resources** > **Network Device Groups** > **All Groups** window.

Table 11: Fields in the Network Device Group Window

Field Name	Usage Guidelines
Name	Enter a name for the root network device group. For all subsequent child network device groups added to this root network device group, enter the name of this newly created network device group. You can have a maximum of six nodes in a network device group hierarchy, including the root node. Each network device group name can have a maximum of 32 characters.
Description	Enter a description for the root or the child network device group.
No. of Network Devices	The number of network devices in the network group is displayed in this column.

Network Device Group Import Settings

The following table describes the fields in the **Import** dialog box in the **Network Device Group** window. To view this window, click the **Menu** icon (≡) and choose **Administration** > **Network Resources** > **Network Device Groups**.

Table 12: Fields in the Network Device Groups Import Window

Field Name	Usage Guidelines
Generate a Template	Click this link to download a CSV template file. Update the template with network device group information in the same format. Save the template locally to import the network device groups into any Cisco ISE deployment.
File	Click **Choose File** and navigate to the location of the CSV file that you want to upload. The file may be new or a file that was exported from another Cisco ISE deployment. You can import network device groups from one Cisco ISE deployment to another, with new and updated network device groups information.
Overwrite Existing Data with New Data	Check this check box if you want to replace the existing network device groups with the device groups in your import file. If you do not check this check box, only the new network device groups in the import file are added to the network device group repository. Duplicate entries are ignored.
Stop Import on First Error	Check this check box to discontinue import at the first instance of encountering an error during the import. If this check box is not checked and an error is encountered, Cisco ISE reports the error and continues importing the rest of the device groups.

Import Templates in Cisco ISE

Cisco ISE allows you to import a large number of network devices and network device groups using CSV files. The template contains a header row that defines the format of the fields. You must not edit this header row except to add columns mentioned in the table below.

Use the **Generate a Template** link in the relevant import flow for network devices and network device groups to download a CSV file to your local system.

Network Devices Import Template Format

The following table lists and describes the fields in the header of the import network device CSV template file.

Table 13: CSV Template Fields and Descriptions for Network Devices

Field	Usage Guidelines
Name:String(32)	Enter a name for the network device. The name must be an alphanumeric string with a maximum of 32 characters.
Description:String(256)	(Optional) Enter a description for the network device with a maximum of 256 characters.

Field	Usage Guidelines
IP Address:Subnets(a.b.c.d/m|...)	Enter the IP address and subnet mask of the network device. You can enter more than one value separated by a pipe (|) symbol.
	IPv4 and IPv6 addresses are supported for network device (TACACS and RADIUS) configurations and for external RADIUS server configurations.
	When you enter an IPv4 address, you can use ranges and subnet masks.
	Ranges are not supported for IPv6.
Model Name:String(32)	Enter the network device's model name with a maximum of 32 characters.
Software Version:String(32)	Enter the network device's software version with a maximum of 32 characters.
Network Device Groups:String(100)	Enter the names of existing network device groups. If it is a subgroup, it must include both the parent and subgroup, separated by a space. The string must be a maximum of 100 characters, for example, *Location>All Location>US*.
Authentication:Protocol:String(6)	Enter the authentication protocol that you want to use. The only valid value is **RADIUS** (not case-sensitive).
Authentication:Shared Secret:String(128)	(Required only if you enter a value in the **Authentication:Protocol:String(6)** field) Enter a string with a maximum of 128 characters.
PasswordEncrypted:Boolean(true|false)	No field value is required for this column.
	If you are importing network devices from Cisco ISE Release 3.3 Patch 1 or earlier releases, you must add a new column with this header to the right of the **Authentication:Shared Secret:String(128)** column, before import. If this column is not added, an error message is displayed, and you will not be able to import the file.
	Network devices with encrypted passwords will be rejected if valid key to decrypt the password is not provided during import.
EnableKeyWrap:Boolean(true|false)	This field is enabled only if KeyWrap is supported in the network device. Enter **true** or **false**.
EncryptionKey:String(ascii:16|hexa:32)	(Required if you enable KeyWrap) Enter the encryption key that is used for session encryption.
	ASCII values: 16 characters (bytes) long.
	Hexadecimal values: 32 characters (bytes) long.
AuthenticationKey:String(ascii:20|hexa:40)	(Required if you enable KeyWrap.) Enter the keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages.
	ASCII values: 20 characters (bytes) long.
	Hexadecimal values: 40 characters (bytes) long.
InputFormat:String(32)	Enter the encryption and authentication keys input format. ASCII and hexadecimal values are accepted.

Field	Usage Guidelines
SNMP:Version:Enumeration (|2c|3)	Enter the version of the SNMP protocol that the profiler service must use—1, 2c, or 3.
SNMP:RO Community:String(32)	(Required if you enter a value in the **SNMP:Version:Enumeration (|2c|3)** field). Enter a string for Read Only Community with a maximum of 32 characters
SNMP:RW Community:String(32)	(Required if you enter a value in the **SNMP:Version:Enumeration (|2c|3)** field). Enter a string for Read Write Community with a maximum of 32 characters.
SNMP:Username:String(32)	Enter a string with a maximum of 32 characters.
	(Required if you enter SNMP version 3 in the **SNMP:Version:Enumeration (|2c|3)** field) Enter **Auth**, **No Auth**, or **Priv**.
SNMP:Authentication Protocol:Enumeration(MD5|SHA)	(Required if you have entered **Auth** or **Priv** for the SNMP security level.) Enter **MD5** or **SHA**.
SNMP:Authentication Password:String(32)	(Required if you have entered **Auth** in the **SNMP:Security Level:Enumeration(Auth|No Auth|Priv)** field.) Enter a string with a maximum of 32 characters.
SNMP:Privacy Protocol:Enumeration(DES|AES128|AES192|AES256|3DES)	(Required if you have entered **Priv** in the **SNMP:Security Level:Enumeration(Auth|No Auth|Priv)** field.) Enter **DES**, **AES128**, **AES192**, **AES256**, or **3DES**.
SNMP:Privacy Password:String(32)	(Required if you have entered **Priv** in the **SNMP:Security Level:Enumeration(Auth|No Auth|Priv)** field.) Enter a string with a maximum of 32 characters.
SNMP:Polling Interval:Integer:600-86400 seconds	Enter the SNMP polling interval, in seconds. A valid value is an integer from 600 to 86400.
SNMP:Is Link Trap Query:Boolean(true|false)	Enable or disable the SNMP link trap by entering **true** or **false**.
SNMP:Is MAC Trap Query:Boolean(true|false)	Enable or disable the SNMP MAC trap by entering **true** or **false**.
SNMP:Originating Policy Services Node:String(32)	Indicate which Cisco ISE server must be used to poll for SNMP data. It is automatic by default, but you can overwrite the setting by assigning different values in this field.
Trustsec:Device Id:String(32)	Enter a Cisco Trustsec device ID, which is a string with a maximum of 32 characters.
Trustsec:Device Password:String(256)	(Required if you have entered a Cisco TrustSec device ID.) Enter a Cisco TrustSec device password, which is a string with a maximum of 256 characters.
Trustsec:Environment Data Download Interval:Integer:1-2147040000 seconds	Enter the Cisco TrustSec environment data download interval. A valid value is an integer from 1 to 2147040000.
Trustsec:Peer Authorization Policy Download Interval:Integer:1-2147040000 seconds	Enter the Cisco TrustSec peer authorization policy download interval. A valid value is an integer from 1 to 2147040000.

Field	Usage Guidelines
Trustsec:Reauthentication Interval:Integer:1-2147040000 seconds	Enter the Cisco TrustSec reauthentication interval. A valid value is an integer from 1 to 2147040000.
Trustsec:SGACL List Download Interval:Integer:1-2147040000 seconds	Enter the Cisco TrustSec security group ACL list download interval. A valid value is an integer from 1 to 2147040000.
Trustsec:Is Other Trustsec Devices Trusted:Boolean(true|false)	Indicate whether a Cisco TrustSec device is trusted by entering **true** or **false**.
Trustsec:Notify this device about Trustsec configuration changes:String(ENABLE_ALL|DISABLE_ALL)	Notify Cisco TrustSec configuration changes to the Cisco TrustSec device by entering **ENABLE_ALL** or **DISABLE_ALL** .
Trustsec:Include this device when deploying Security Group Tag Mapping Updates:Boolean(true|false)	Indicate if the Cisco TrustSec device is included in security group tag by entering **true** or **false**.
Deployment:Execution Mode Username:String(32)	Enter the user name that has privileges to edit the network device configuration. It is a string with a maximum of 32 characters.
Deployment:Execution Mode Password:String(32)	Enter the device password, which is a string with a maximum of 32 characters.
Deployment:Enable Mode Password:String(32)	Enter the password of the device that allows you to edit its configuration. It is a string with a maximum of 32 characters.
Trustsec:PAC issue date:Date	Enter the issuing date of the last Cisco TrustSec PAC that was generated by Cisco ISE for the Cisco TrustSec device.
Trustsec:PAC expiration date:Date	Etner the expiration date of the last Cisco TrustSec PAC that was generated by Cisco ISE for the Cisco TrustSec device.
Trustsec:PAC issued by:String	Enter the name of the issuer (a Cisco TrustSec administrator) of the last Cisco TrustSec PAC that was generated by Cisco ISE for the Cisco TrustSec device. It must be a string value.

Network Device Groups Import Template Format

The following table lists the fields in the template header and provides a description of the fields in the Network Device Group CSV file.

Table 14: CSV Template Fields and Descriptions for Network Device Groups

Field	Description
Name:String(100):	(Required) This field is the network device group name. It is a string with a maximum of 100 characters in length. The full name of an NDG can have a maximum of 100 characters in length. For example, if you create a subgroup India under the parent groups Global > Asia, then the full name of the NDG that you create would be Global#Asia#India. The full name cannot exceed 100 characters in length. If the full name of the NDG exceeds 100 characters in length, the NDG creation fails.

Field	Description
Description:String(1024)	This is an optional field. It is a string, with a maximum of 1024 characters in length.
Type:String(64):	(Required) This field is the network device group type. It is a string, with a maximum of 64 characters in length.
Is Root:Boolean(true|false):	(Required) This is a field that determines if the specific network device group is a root group. Valid value is true or false.

IPsec Security to Secure Communication Between Cisco ISE and NAD

IPsec is a set of protocols that provides security to IP. The RADIUS, and TACACS+ protocols use the MD5 hashing algorithm. For greater security, Cisco ISE offers the IPsec feature. IPsec provides secure communication by authenticating the sender, discovering any changes in data during transmission, and encrypting the data that is sent.

Cisco ISE supports IPsec in tunnel and transport modes. When you enable IPsec on a Cisco ISE interface and configure the peers, an IPsec tunnel is created between Cisco ISE and the NAD to secure the communication.

You can define a pre-shared key or use X.509 certificates for IPsec authentication. IPsec can be enabled on Gigabit Ethernet 1 through Gigabit Ethernet 5 interfaces. You can configure IPsec on only one Cisco ISE interface per PSN.

Note IPsec is only supported on Bond 1 and Bond 2 interfaces. Gigabit Ethernet 0 and Bond 0 (when Gigabit Ethernet 0 and Gigabit Ethernet 1 interfaces are bonded) are management interfaces in the Cisco ISE CLI. IPsec is not supported on Gigabit Ethernet 0 and Bond 0. Information about bond interfaces is not displayed in the IPsec page in the Cisco ISE GUI.

Cisco ISE Releases 2.2 and later support IPsec.

For more information on IPsec configuration, restrictions, and support, see the Security Configuration Guide, Cisco IOS XE Cupertino 17.7.x (Catalyst 9300 Switches).

From Cisco ISE Release 3.4, you can configure IPsec on Cisco ISE PSN nodes using only native IPsec. For information on how to configure native IPsec, see Configure Native IPsec on Cisco ISE.

For information on how to migrate from Legacy IPsec (ESR) to Native IPsec, see Migrate from Legacy IPsec to Native IPsec on Cisco ISE, on page 37 in the *Cisco ISE Administrator Guide*.

Configure Native IPsec on Cisco ISE

The native IPsec configuration can be used to establish security associations between Cisco ISE PSNs and NADs across an IPsec tunnel using IKEv1 and IKEv2 protocols.

![Note icon]

Note
- Ensure that the IPsec configurations on the PSNs of Cisco ISE and the NADs are the same.

- Each PSN can support 150 IPsec tunnels (inclusive of VTI).

Before you begin

To configure Native IPsec in Cisco ISE, you'll need the following.

In Cisco ISE:

- Ensure that you have a Cisco ISE Essentials License.

- (Optional) If you're using the **X.509 Certificates** option, upload a system certificate for IPsec for every PSN that will establish a native IPsec connection. Check the **IPsec: Use certificate for Native IPsec** check box in the **System Certificates** window. You must also upload CA certificates for the Cisco ISE IPsec system certificate and the NAD certificate to the trust store. Check the **Trust for authentication within ISE** check box in the CA IPsec Trusted Certificate in the **Trusted Certificates** window.

☞

Important   Cisco ISE 3.3 Patch 2 onwards, you will be able to establish the IPsec tunnel using the **X.509 Certificates** option only if all the associated peer and intermediate CA certificates contain either the Authority Information Access (AIA) OCSP URL(s) or the crlDistributionPoint URL(s) or both. Existing certificates must be updated to include the AIA OCSP URL(s) or the crlDistributionPoint URL(s) or both, to be able to continue using this option. If AIA or crlDistributionPoint information is not present in the certificates, you can use only the **Pre-shared Keys** option to establish the IPsec tunnel.

- Add a NAD with a specific IP address in the **Network Devices** window.

- Configure IPsec on the NAD. The IPsec configuration on the Cisco ISE PSN and the NAD must be the same.

Step 1   In the Cisco ISE GUI, hover over **Administration** and navigate to **System** > **Settings** > **Protocols** > **IPsec** > **Native IPsec**.

Step 2   Click **Add** to configure a security association between a Cisco ISE PSN and a NAD.

Step 3   In the **Node-Specific Settings** section, enter the following details:

a) From the **Select Node** drop-down list, choose the required Cisco ISE PSN.
b) In the **NAD IP Address** field, enter the corresponding value.
c) From the **Native IPsec Interface** drop-down list, choose the required native IPsec traffic interface.
d) (Optional) Check the **Configure VTI** checkbox to configure a virtual tunnel interface (VTI).

- In the **Remote Tunnel IP address** field, enter the corresponding value.

- In the **Local Tunnel IP address** field, enter the corresponding value.

Note   Following an upgrade to Cisco ISE Release 3.4, all IPsec connections must be disabled and re-enabled from the Cisco ISE GUI to ensure that all existing VTI tunnels are active.

Step 4   In the **Authentication Settings** section, click the radio button to choose one of the following authentication types for the selected Cisco ISE PSN node:

   a) **Pre-shared Key**: If you choose this option, you must enter the preshared key and configure the same key on the network device. Use alphanumeric characters for the preshared key. Special characters aren't supported. For instructions on how to configure the preshared key on the network device, see the network device documentation.

   b) **X.509 Certificates**: From the **X.509 Certificates** drop-down list, choose the required X.509 certificate for the IPsec tunnel.

      Note   Configure the required certificates (IPsec System Certificate and CA IPsec Trusted Certificate) before choosing the **X.509 Certificates** option. The certificates must contain the SAN (Subject Alternate Name) extension and the DNS.

      If the certificates are added or modified after the correlated Native IPsec configuration is in place, the Native IPsec configuration needs to be saved again.

Step 5   In the **General Settings** section, enter the following details:

   a) From the **IKE Version** drop-down list, choose the required IKE version.

   b) From the **Mode** drop-down list, choose the required mode.

      If you are configuring VTI, only the tunnel mode is supported.

   c) From the **ESP/AH Protocol** drop-down list, choose the required protocol.

   d) (Optional) In the **IKE Reauth Time** field, enter a corresponding value.

      The **IKE Reauth Time** value ranges 0–86400. You can disable the **IKE Reauth Time** field by entering the value as 0 in the field.

Step 6   In the **Phase One Settings** section, you can configure IKE Security Association Configuration security settings to protect communications between two IKE daemons:

   a) From the **Encryption Algorithm** drop-down list, choose the required encryption algorithm.

   b) From the **Hash Algorithm** drop-down list, choose the required Hash algorithm.

   c) From the **DH Group** drop-down list, choose the required DH group.

   d) (Optional) In the **Re-key Time** field, enter a corresponding value.

      The **Re-key Time** value ranges 0–86400. You can disable the **Re-key Time** field by entering the value as 0 in this field.

Step 7   In the **Phase Two Settings** section, you can configure the Native IPsec security association configuration security settings to protect the IP traffic between two endpoints. Enter the following details:

   a) From the **Encryption Algorithm** drop-down list, choose the required encryption algorithm.

   b) From the **Hash Algorithm** drop-down list, choose the required Hash algorithm.

   c) (Optional) From the **DH Group** drop-down list, choose the required DH group.

   d) (Optional) In the **Re-key Time** field, enter a corresponding value.

      The **Re-key Time** value ranges 0–2592000. You can disable the **Re-key Time** field by entering the value as 0 in the field.

Step 8   Click **Save** to activate Native IPsec on the chosen Cisco ISE PSN node.

Note
- Multiple Cisco ISE interfaces should not be configured in the same IP subnet while configuring Native IPsec.

- When an IP address is changed on an existing IPsec tunnel interface, you must re-enable the existing tunnel configuration to reflect the change in the IP address.

- If an existing interface of an IPsec tunnel gets shut down, the IPsec status for that tunnel will be displayed as **Established** until the next re-key or reauthentication takes place.

- To view audit reports related to Native IPsec, choose **Operations** > **Reports** > **Audit** > **Change Configuration Audit**.

View and Modify Native IPsec Configurations in Cisco ISE

You can add, view, edit, duplicate, disable, and remove the security associations established between Cisco ISE PSNs and NADs through the Native IPsec configuration in the **Native**IPsec **Configuration** window.

You can filter through the Native IPsec configurations using quick filters.

You can add more columns to the **Native** IPsec **Configuration** table. Click the gear icon on the top-right of the **Native** IPsec **Configuration** table and choose the columns of your choice from columns such as Phase-one Encryption Algorithm, Phase-two Encryption Algorithm, Phase-one Hash Algorithm, and so on, and click **Go** to add the chosen columns to the **Native** IPsec **Configuration** table.

Migrate from Legacy IPsec to Native IPsec on Cisco ISE

From Cisco ISE Release 3.4, legacy IPsec (ESR) is not supported on Cisco ISE. All IPsec configurations on Cisco ISE will be native IPsec configurations. We recommend that you migrate to native IPsec from legacy IPsec (ESR) before upgrading to Cisco ISE Release 3.4 to avoid any loss of tunnel and tunnel configurations.

Before you begin

To migrate from legacy IPsec to native IPsec in Cisco ISE, you need the following:

- Legacy IPsec (ESR) configuration backup

- Keys and certificates of Legacy IPsec (ESR)

Step 1 Back up legacy IPsec (ESR) configuration:
   a) Log in to the Cisco ISE CLI ESR shell and save the running configuration on a file in bootflash.
   b) Export the running configuration file to your computer using SCP or FTP. You can use this saved ESR configuration file as your ESR configuration backup.

Step 2 Export IPsec configuration:
   a) Export the keys and certificates from Legacy IPsec (ESR). For more information on exporting keys and certificates in Cisco ISE, see Backup and Restoration of Cisco ISE CA Certificates and Keys.
   b) From the Cisco ISE CLI ESR shell, execute the **show runnning config** command to view the running configuration and crypto settings.

c) Compare the crypto settings configured on your legacy IPsec (ESR) with the references given in Table 15: Compare Legacy IPsec Configuration and Native IPsec Configuration: Phase One Settings and Table 16: Compare Legacy IPsec Configuration and Native IPsec Configuration: Phase Two Settings.

Table 15: Compare Legacy IPsec Configuration and Native IPsec Configuration: Phase One Settings and Table 16: Compare Legacy IPsec Configuration and Native IPsec Configuration: Phase Two Settings show a direct comparison between the legacy IPsec (ESR) CLI commands and their corresponding counterparts for native IPsec configuration in the Cisco ISE GUI. You can use the Legacy IPsec (ESR) configuration information to configure Native IPsec on Cisco ISE.

Table 15: Compare Legacy IPsec Configuration and Native IPsec Configuration: Phase One Settings

show running config command on Legacy IPsec (ESR)	Native IPsec Configuration in the Cisco ISE GUI

• **crypto isakmp policy 10**
 	
• **encr aes**
 	
• **hash sha256**
 	
• **authentication pre-share**
 	
• **group 14**
 	
• **crypto isakmp key cisco123 address 0.0.0.0**
	• **Authentication Settings**: Pre-share
	
	• **Pre-share Key**: cisco123
	
	• **IKE Version**: IKEv1
	
	• **Phase-One Settings**
	    • **Encryption Algorithm**: AES-128
	    • **Hash Algorithm**: SHA-256
	    • **DH Group**: Group-14

Table 16: Compare Legacy IPsec Configuration and Native IPsec Configuration: Phase Two Settings

show running config command on Legacy IPsec (ESR)	Native IPsec Configuration in the Cisco ISE GUI

• **crypto IPsec transform-set IPsec-ts esp-aes esp-sha256-hmac mode tunnel**
 	
• **crypto map IPsec-crypto-map 10 IPsec-isakmp**
 	
• **set peer 192.168.10.1**
 	
• **set transform-set IPsec-ts**
 	
• **set pfs group14**
 	
• **match address 100**
	• **ESP/AH Protocol**: ESP
	
	• **Mode**: Tunnel
	
	• **Phase-Two Settings**
	    • **Encryption Algorithm**: AES-128
	    • **Hash Algorithm**: SHA-256
	    • **DH Group**: Group-14

Step 3   Disable legacy IPsec (ESR):

a) In the Cisco ISE GUI, hover your cursor over **Administration** and navigate to **System** > **Settings** > **Protocols** > **IPsec** > **Legacy IPsec (ESR)**.

b) Check the check box to select the Cisco ISE nodes on which legacy IPsec (ESR) must be disabled.

c) Click the **Disable** radio button in the **Enable/Disable IPsec for Selected Nodes** field.

This disables IPsec on the selected nodes and restarts Cisco ISE.

d) From the Cisco ISE admin CLI, execute the **ISE/admin#show esr status** command to verify that the ESR status of the chosen Cisco ISE node is disabled. The following output is displayed:

% ESR 5921 is disabled.

e) (Optional) From the Cisco ISE admin CLI, execute the **ISE/admin#esr** command to verify whether the ESR shell is disabled.

f) From the Cisco ISE admin CLI, execute the **ISE/admin#show interface** command to verify whether the IP address is restored on the Cisco ISE interface. The following output is displayed:

GigabitEthernet 1 flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 192.168.10.11 netmask 255.255.255.0 broadcast 192.168.10.255 inet6 fe80::250:56ff:fe92:5f13 prefixlen 64 scopeid 0x20<link>.

Step 4 Enable native IPsec:

a) In the Cisco ISE GUI, hover your cursor over **Administration** and navigate to **Network Resources** > **Network Devices**.

b) Select the NAD that was previously selected for legacy IPsec (ESR) configuration for native IPsec configuration too.

c) Click **Edit** to edit the IPsec details of the NAD.

d) From the **Legacy IPsec (ESR)** drop-down list in the **Network Device Group** section, choose **No**.

e) Click **Save**.

f) Configure native IPsec to establish a security association between Cisco ISE PSN and chosen NAD across an IPsec tunnel using IKEv1 and IKEv2 protocols. For information on how to configure native IPsec, see .

Mobile Device Manager Interoperability with Cisco ISE

Mobile Device Management (MDM) servers secure, monitor, manage, and support mobile devices that are deployed across mobile operators, service providers, and enterprises. Traditionally, MDM servers have only supported mobile devices. Some MDM servers now manage all types of devices in a network (mobile phones, tablets, laptops, and desktops) and are called Unified Endpoint Management (UEM) servers. MDM servers act as a policy server that controls the use of some applications on a mobile device (for example, an email application) in the deployed environment. Cisco ISE queries a connected MDM server for information about various attributes that you can use to create network authorization policies.

You can run multiple active MDM servers on your network, from different vendors. This allows you to route different endpoints to different MDM servers based on device factors such as location or device type.

Cisco ISE also integrates with MDM servers using the Cisco MDM Server Info APIs, Version 2 and later versions, to allow devices to access the network over VPN via Cisco AnyConnect 4.1 and Cisco Adaptive Security Appliances 9.3.2 or later.

In the following illustration, Cisco ISE is the enforcement point and the MDM policy server is the policy information point. Cisco ISE obtains data from the MDM server to provide a complete solution.

Figure 3: MDM Interoperability with Cisco ISE
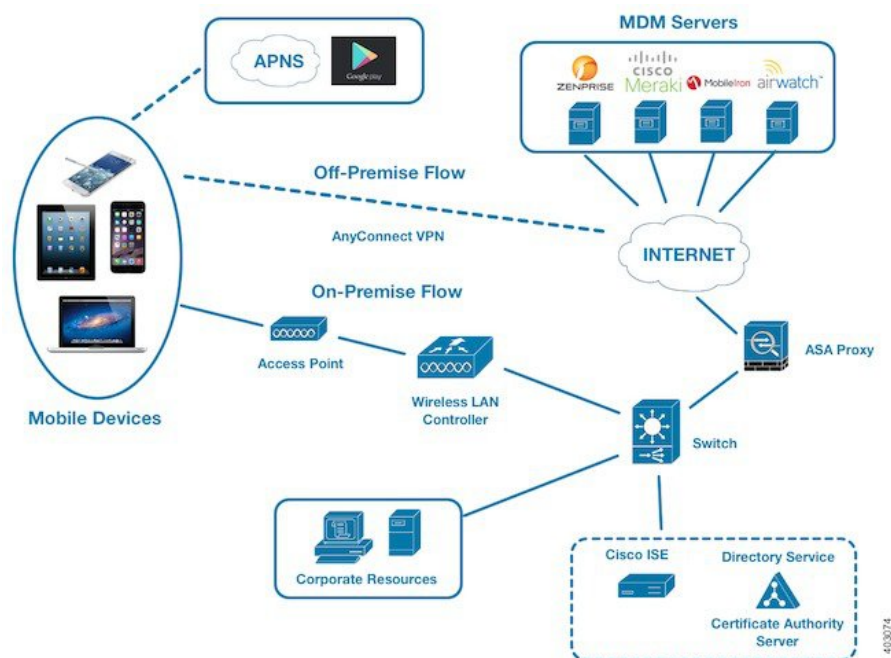
Configure Cisco ISE to interoperate with one or more external MDM servers. By setting up this type of third-party connection, you can use the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. Cisco ISE applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points. The policies give you greater control of the remote devices that are accessing the Cisco ISE-enabled network.

For a list of the MDM vendors supported by Cisco ISE, see Supported Unified Endpoint Management and Mobile Device Management Servers, on page 43.

Supported Mobile Device Management Use Cases

Cisco ISE performs the following functions with external MDM servers:

- Manages device registration: Unregistered endpoints that access the network are redirected to a registration page that is hosted on the MDM server. Device registration includes the user role, device type, and so on.

- Handles device remediation: Endpoints are granted restricted access during remediation.

- Augments endpoint data: The endpoint database is updated with information from the MDM server that you cannot gather using the Cisco ISE profiling services. Cisco ISE uses multiple device attributes that you can view in the **Endpoints** page. In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Work Centers** > **Network Access** > **Identities** > **Endpoints**.

  The following are examples of the device attributes available.

- MDMImei: xx xxxxxx xxxxxx x

- MDMManufacturer: Apple

- MDMModel: iPhone

- MDMOSVersion: iOS 6.0.0

- MDMPhoneNumber: 5550100

- MDMSerialNumber: DNPGQZGUDTFx

- Polls the MDM server every four hours for device compliance data. Configure the polling interval in the **External MDM Servers** page. (To view this page, click the **Menu** icon (≡) and choose **Work Centers** > **Network Access** > **Network Resources** > **External MDM Servers**.

- Issues device instructions through the MDM server: Cisco ISE issues remote actions for user devices through the MDM server. Initiate remote actions from the Cisco ISE administration portal through the **Endpoints** page. To view this page, click the **Menu** icon (≡) and choose **Context Visibility** > **Endpoints**. Check the check box next to the MDM server and click **MDM Actions**. Choose the required action from the drop-down list displayed.

Vendor MDM Attributes

When you configure an MDM server in Cisco ISE, Cisco ISE queries the MDM server for device attribute information and adds the information to the MDM system dictionary. The following attributes are used for registration status, and are commonly supported by MDM vendors.

Cisco ISE uses APIs to query MDM servers for the required device attributes. Cisco ISE Release 3.1 and later releases support MDM APIs Version 3. The Version 3 APIs include APIs that allow Cisco ISE to send queries to MDM servers for device attributes that help Cisco ISE identify endpoints that use MAC address randomization. Cisco ISE queries the MDM server for the following attributes:

- GUID: A unique device identifier that replaces the use of MAC address to identify a device.

- MAC addresses: The list of MAC addresses that a UEM or MDM server has recorded for a particular device. A maximum of five MAC addresses are shared for a device.

If an MDM server does not provide values for the required attributes, Cisco ISE fills the attributes fields with the default values that are mentioned in the following table.

Table 17: MDM Attributes and Values

Attribute Name	Attribute Dictionary	Default Value	Data That is Expected From UEM or MDM Servers	Data That is Expected From Microsoft SCCM Servers
DaysSinceLastCheckin Supported from MDM API Version 3	MDM	None	The number of days since a user has last checked in or synchronized a device with the UEM or MDM server. The valid range is 1–365 days.	The number of days since a user has last checked in or synchronized a device with the SCCM server. The valid range is 1–365 days.
DeviceCompliantStatus	MDM	NonCompliant	**Compliant** or **NonCompliant**.	**Compliant** or **NonCompliant**.

Attribute Name	Attribute Dictionary	Default Value	Data That is Expected From UEM or MDM Servers	Data That is Expected From Microsoft SCCM Servers
DeviceRegisterStatus	MDM	UnRegistered	**Registered** or **UnRegistered**.	**Registered** or **UnRegistered**.
DiskEncryptionStatus	MDM	Off	**On** or **Off**.	**On** or **Off**.
IMEI	MDM	None	The IMEI number of the device.	Not applicable.
JailBrokenStatus	MDM	Unbroken	**Reachable** or **UnReachable**.	**Reachable** or **UnReachable**.
MDMFailureReason	MDM	None	The device failure reason.	The device failure reason.
MDMServerName	MDM	None	The name of the server.	The name of the server.
MDMServerReachable	MDM	Reachable	**Reachable** or **UnReachable**.	**Reachable** or **UnReachable**.
MEID	MDM	None	The MEID value of the device.	Not applicable.
Manufacturer	MDM	None	The name of the device manufacturer.	Not applicable.
Model	MDM	None	The name of the device model.	Not applicable.
OsVersion	MDM	None	The operating system version of the device.	Not applicable.
PhoneNumber	MDM	None	The phone number of the device.	Not applicable.
PinLockStatus	MDM	Off	**On** or **Off**.	Not applicable.
SerialNumber	MDM	None	The serial number of the device.	Not applicable.
ServerType	MDM	None	**MDM** for a Mobile Device Manager server. **DM** for Desktop Device Manager server.	**DM** for Desktop Device Manager server.
UDID	MDM	None	The UDID number of the device.	Not applicable.
UserNotified	MDM	No	**Yes** or **No**	Not applicable.

Attribute Name	Attribute Dictionary	Default Value	Data That is Expected From UEM or MDM Servers	Data That is Expected From Microsoft SCCM Servers
GUID Supported from MDM API Version 3	Not a Dictionary attribute	None	The GUID is a unique device identifier that is used to identify a device instead of the device's MAC address, UDID, MEID, or IMEI values. The GUID template is **ID:MDMServer:GUID:{{DeviceId}}** The GUID value is generated and provided by the MDM server, not by Cisco ISE.	Not applicable.
Macaddresses Supported from MDM API Version 3	Not a Dictionary attribute	None	The list of MAC addresses that the UEM or MDM server has recorded for a particular device. A maximum of five MAC addresses can be shared for a device. The Macaddresses values are generated and provided by the MDM server, not by Cisco ISE.	Not applicable.

If a vendor's unique attributes are not supported, you may be able to use ERS APIs to exchange vendor-specific attributes. Check the vendor's documentation for information on the ERS APIs that are supported.

The new MDM dictionary attributes are available for use in authorization policies.

Supported Unified Endpoint Management and Mobile Device Management Servers

Supported MDM servers include products from the following vendors:

- Absolute
- Blackberry - BES
- Blackberry - Good Secure EMM
- Cisco Meraki Systems Manager
- Citrix XenMobile 10.x (On-prem)
- Globo
- IBM MaaS360

- Ivanti (previously MobileIron UEM), core and cloud UEM services

For the use case of handling random and changing MAC Addresses in Cisco ISE 3.1, you must integrate MobileIron Core 11.3.0.0 Build 24 and later releases to receive GUID values.

✎

Note Some versions of MobileIron do not work with Cisco ISE. MobileIron is aware of this problem, and have a fix. Contact MobileIron for more information.

- JAMF Casper Suite

- Microsoft Endpoint Configuration Manager

- Microsoft Endpoint Manager Intune

- Mosyle

- SAP Afaria

- Sophos

- SOTI MobiControl

- Symantec

- Tangoe

- VMware Workspace ONE (earlier known as AirWatch)

- 42Gears

For the configurations that you must perform in your endpoint management servers to integrate the servers with Cisco ISE, see Integrate UEM and MDM Servers With Cisco ISE.

ISE Community Resource

How To: Meraki EMM / MDM Integration with ISE

Ports Used by the Mobile Device Management Server

The following table lists the ports that must be open between Cisco ISE and an MDM server to enable them to communicate with each other. See the documentation from the MDM vendor for a list of ports that must be open on the MDM agent and server.

Table 18: Ports Used by the MDM Server

MDM Server	Ports
MobileIron	443
Citrix XenMobile 10.x (On-prem)	443
Blackberry - Good Secure EMM	19005

MDM Server	Ports
VMware Workspace ONE (earlier known as AirWatch)	443
SAP Afaria	443
IBM MaaS360	443
Cisco Meraki	443
Microsoft Intune	80 and 443
Microsoft SCCM	80 and 443

Mobile Device Management Integration Process Flow

1. The user associates a device with an SSID.

2. Cisco ISE makes an API call to the MDM server.

3. This API call returns a list of devices for the user and the posture statuses for the devices.

   Note   The input parameter is the MAC address of the endpoint device. For off-premise Apple iOS devices (any device that connects to Cisco ISE through a VPN), the input parameter is the UDID.

4. If the user's device is not on this list, it means that the device is not registered. Cisco ISE sends an authorization request to the NAD to redirect to Cisco ISE. The user is presented with the MDM server page.

5. Cisco ISE uses MDM to provision the device and presents the appropriate window for the user to register the device.

6. The user registers the device in the MDM server, and the MDM server redirects the request to Cisco ISE through automatic redirection or manual browser refresh.

7. Cisco ISE queries the MDM server again for the posture status.

8. If the user's device is not compliant with the posture (compliance) policies that are configured on the MDM server, the user is notified that the device is out of compliance. The user must take the necessary action to ensure that the device is compliant.

9. When the user's device is compliant, the MDM server updates the device's state in its internal tables.

10. If the user refreshes the browser now, the control is transferred back to Cisco ISE.

11. Cisco ISE polls the MDM server every four hours to get compliance information and issues the appropriate Change of Authorization (CoA). You can configure the polling interval. Cisco ISE also checks the MDM server every five minutes to make sure that it is available.

Figure 4: The MDM Process Flow in Cisco ISE
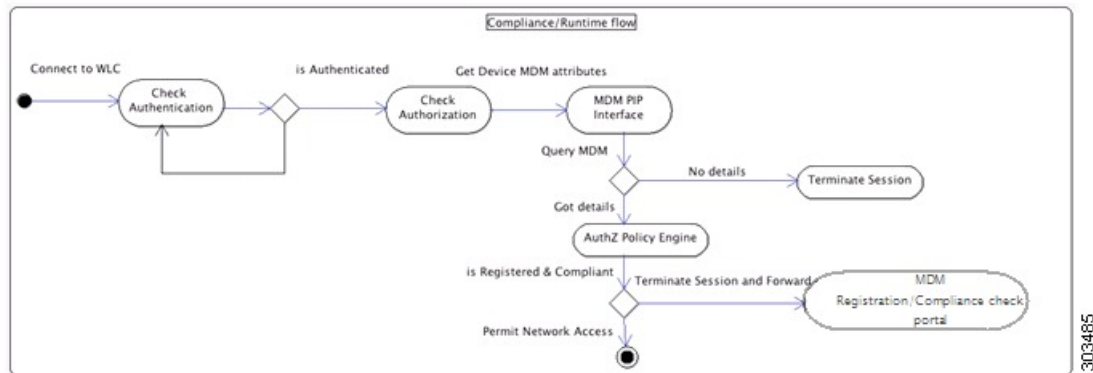
Note   A device can only be enrolled in a single MDM server at a time. If you want to enroll the same device to an MDM service from another vendor, the previous vendor's profiles must be removed from the device. The MDM service usually offers a "corporate wipe", which only deletes the vendor's configuration from the device (not the whole device). The user can also remove the files. For example, on an iOS device, the user can go to the **Settings** > **General** > **Device management** window, and click **Remove Management**. Or the user can go to the MyDevices portal in Cisco ISE and click **Corporate Wipe**.

Handle Random and Changing MAC Addresses with Mobile Device Management Servers

Configure Cisco ISE to identify endpoints that are connected to an MDM server by a unique device identifier instead of a MAC address, to avoid issues that are caused by the use of random and changing MAC addresses. As a privacy measure, mobile devices increasingly use random and changing MAC addresses for each SSID that they connect to. Some desktop operating systems offer users the ability to randomize MAC addresses at regular intervals as well. This means that an endpoint presents different MAC addresses to the MDM server and Cisco ISE. As a result, when the MDM server and Cisco ISE are integrated and an action is initiated for an endpoint, issues arise because of the difference in the endpoint identity in the two systems.

To work around this issue, you can configure Cisco ISE to use a unique device identifier instead of MAC addresses. When an endpoint enrolls with an MDM server, the MDM server sends a certificate with a GUID value to the endpoint. The endpoint uses this certificate for authentication with Cisco ISE. Cisco ISE receives the GUID for the endpoint from the certificate. All communications between Cisco ISE and the MDM server now use the GUID to identify the endpoint, ensuring accuracy and consistency between the two systems.

Note that GUID is available only in certificate-based authentication methods. You must configure the certificates issued by the MDM or UEM server to include the GUID in the SAN URI or CN fields. We recommend configuring the SAN URI field for GUID. If the same certificate is used to authenticate an endpoint connected to Active Directory, the presence of GUID in the CN field might cause issues.

Basic authentication methods that only use username and password will not be able to leverage the GUID-based solution.

For the reauthentication of endpoints with MAC address and GUID through the EAP-TLS protocol, the transaction per second (TPS) for updating context visibility services is 12–15 endpoints per second.

The Cisco ISE MDM APIs have been updated (Cisco ISE MDM APIs Version 3) to facilitate the gathering and management of GUID data.

Configure GUID for Connected MDM Servers

To check if an MDM server you have already connected to Cisco ISE supports the latest Cisco ISE MDM APIs and can send GUID information, carry out the following steps:

1. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **External MDM**.

2. In the **MDM Servers** window, check the check box for the MDM server you want to update, and click **Edit**.

3. Click **Test Connection**.

4. If the MDM server supports Cisco ISE MDM APIs Version 3, a new section called **Device Identifiers** is displayed.

   Check the check boxes for one or more of the following options that you want to enable:

   - **Cert - SAN URI, GUID**

   - **Cert - CN, GUID**

   - **Legacy MAC Address**

   You can drag and drop the options to organize them in the order of preference. For example, if you place **Cert - SAN URI, GUID** first and then **Cert - CN, GUID**, Cisco ISE first queries the MDM server for the SAN URI and GUID attributes of an endpoint. If the requested attributes are not available, Cisco ISE queries for the common name and GUID attributes of the endpoint.

5. Click **Save**.

Sharing GUID Through pxGrid

Cisco ISE can share this GUID information through the pxGrid with other Cisco solutions. For example, you can share the GUID received from MDM servers with a Catalyst Center in your deployment through pxGrid topics.

Set Up Mobile Device Management Servers with Cisco ISE

To set up MDM servers with Cisco ISE, you must perform the following high-level tasks:

Step 1 Import the MDM server certificate into Cisco ISE, except for Intune, where you import the Policy Administration node's (PAN) certificate into Azure.

Step 2 Create mobile device manager definitions.

Step 3 Configure ACLs on the Cisco WLCs.

Step 4 Configure an authorization profile that redirects nonregistered devices to the MDM server.

Step 5 If there are multiple MDM servers on the network, configure separate authorization profiles for each vendor.

Step 6 Configure authorization policy rules for the MDM use cases.

Import Mobile Device Management Server Certificate into Cisco ISE

For Cisco ISE to connect with the MDM server, you must import the MDM server certificate into the Cisco ISE Trusted Certificates store. If your MDM server has a CA-signed certificate, you must import the root certificate into the Cisco ISE Trusted Certificates store.

> **Note** For Microsoft Azure, import the Cisco ISE certificate into Azure. See Connect Microsoft Intune to Cisco ISE as a Mobile Device Management Server.

Step 1 Export the MDM server certificate from your MDM server and save it on your local machine.

Step 2 In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration** > **System** > **Certificates** > **Trusted Certificate** > **Import**.

Step 3 In the **Import a new Certificate into the Certificate Store** window, click **Choose File** to select the MDM server certificate that you obtained from the MDM server.

Step 4 Add a name for the certificate in the **Friendly Name** field.

Step 5 Check the **Trust for authentication within ISE** check box.

Step 6 Click **Submit**.

Step 7 Verify that the **Trust Certificates** window lists the newly added MDM server certificate.

Define Device Management Servers in Cisco ISE

Define mobile and desktop device management servers in Cisco ISE to allow Cisco ISE to communicate with the required servers. You can configure the authentication type that is used to communicate with the servers, the frequency at which Cisco ISE requests device information from a device management server, and so on.

To define a mobile management server, see Configure Mobile Device Management Servers in Cisco ISE, on page 48.

To define a Microsoft System Center Configuration Manager (SCCM) server, see Select Configuration Baseline Policies for Endpoint Compliance from Desktop Device Manager Server.

Configure Mobile Device Management Servers in Cisco ISE

The first MDM server that provides an endpoint's information to Cisco ISE is displayed in the endpoint information in the **Context Visibility** > **Endpoints** window. The MDM server information is not automatically updated when an endpoint connects with a different MDM server. You must delete the endpoint from the **Context Visibility** window, and then the endpoint must reconnect with an MDM server, for the **Context Visibility** window to display the updated information.

The following image displays the Cisco ISE GUI fields that you must work with during this task. The numbers in the image correspond to the step numbers in the following task.

Figure 5: Add an MDM Server in Cisco ISE

Step 1   In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration** > **Network Resources** > **External MDM**.

Step 2   In the **MDM / UEM Integrations** window, click **Add**.

Step 3   Enter the name and description of the MDM server that you want to add in the corresponding fields.

Step 4   From the **Server Type** drop-down list, choose **Mobile Device Manager**.

Step 5   From the **Authentication Type** drop-down list, choose either **Basic** or **OAuth - Client Credentials**.

If you choose the **Basic** authentication type, the following fields are displayed:

- **Host Name / IP Address**: Enter the hostname or IP address of the MDM server.

- **Port**: Specify the port to be used when connecting to the MDM server, which is usually 443.

- **Instance Name**: If this MDM server has several instances, enter the instance that you want to connect to.

- **Username**: Enter the username that must be used to connect to the MDM server.

- **Password**: Enter the password that must be used to connect to the MDM server.

If you choose the **OAuth - Client Credentials** authentication type, the following fields are displayed:

- From the **Auto Discovery** drop-down list, choose **Yes** or **No**.

- **Auto Discovery URL**: Enter the value of Microsoft Azure AD Graph API Endpoint from the Microsoft Azure management portal. This URL is the endpoint at which an application can access directory data in your Microsoft Entra ID using the Graph API. For more information, see Integrate MDM and UEM Servers with Cisco ISE.

- **Client ID**: The unique identifier for your application. Use this attribute if your application accesses data in another application, such as the Microsoft Azure AD Graph API, Microsoft Intune API, and so on.

- **Token Issuing URL**: Enter the value of the Oauth2.0 Authorization Endpoint. This is the endpoint from which Cisco ISE obtains an access token using OAuth2.0.

- **Token Audience**: The recipient resource that the token is intended for, which is a public, well-known **APP ID URL** to the Microsoft Intune API.

Polling Interval: Enter the polling interval, in minutes, for Cisco ISE to poll the MDM server for noncompliant endpoints. Set this value to match the polling interval on your MDM server. The valid range is from 15 to 1440 minutes. The default value is 240 minutes. We recommend that you set the polling interval more than 60 minutes in production environments to minimize any performance impact that might occur due to large numbers of noncompliant endpoints.

ISE retrieves list of non compliant devices information through MAC Address/GUID based non compliant API calls (Eg:)

Since this is a bulk retrieval API, ISE uses paging info provided by MDM Server.

ISE updates endpoint records compliance information based on the non compliance API response. If ISE finds active sessions on these non compliance devices, then it will reauthorize.

ISE limits the non compliance API calls to maximum of 200 requests or 20,000 endpoint records, whichever happens first.

If you set the polling interval to 0, Cisco ISE disables polling with the MDM server.

Note   Cisco ISE limits API calls from noncompliant endpoints to 200. If the external MDM server receives requests from more than 20000 noncompliant endpoints, the external MDM server polling interval is automatically set to 0. You also receive the following alarm on Cisco ISE:

```
MDM Compliance Polling Disabled: Reason is Periodic Compliance Polling received huge
non-compliance device information.
```

MDM / UEM Device Compliance Timeout: Enter the timeout duration, in milliseconds, for which Cisco ISE waits for a response from the MDM or UEM server after querying that MDM or UEM server. The default value is 30000 milliseconds. You can set a value 1–30000 milliseconds if you want to query only one MDM or UEM server. If you want to query multiple MDM or UEM servers using device-compliance APIs, you must set a value less than 300 milliseconds to avoid impact on system performance.

Step 6   From the **Status** drop-down list, choose **Enabled**.

Step 7   To verify whether the MDM server is connected to Cisco ISE, click **Test Connection**. Note that **Test Connection** is not intended to check permissions for all the use cases (get baselines, get device information, and so on). These are validated when the server is added to Cisco ISE.

Figure 6: Add an MDM Server in Cisco ISE

If the MDM server you are configuring supports Cisco ISE MDM API Version 3 and can share the attribute GUID with Cisco ISE, the **Device Identifiers** area is displayed. For more information, see Handle Random and Changing MAC Addresses with Mobile Device Management Servers, on page 46.

Check the check boxes for one or more of the following options that you want to enable, and arrange them in the order of preference by dragging and dropping each option in its place:

- **Cert - SAN URI, GUID**

- **Cert - CN, GUID**

- **Legacy MAC Address**

Step 8　　Click **Save**.

Configure General MDM or UEM Settings

Configure the general MDM or UEM settings to allow Cisco ISE to query multiple MDM or UEM servers and identify the MDM or UEM server to which an endpoint is connected.

For example, when a new endpoint is registered in Intune, you need a few conditions, such as, device type or user type in the authorization policy for Cisco ISE, to evaluate Intune for the endpoints.

If you enable the **Query Multiple MDM / UEM Integrations** option, Cisco ISE queries all the MDM servers listed in the authorization policy and identifies the server to which the endpoint is registered.

Figure 7: Sample Authorization Policy with Multiple MDM Servers

Step 1　　In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **General MDM / UEM Settings**.

Step 2　　In the **General MDM / UEM Settings** window, click **Query Multiple MDM / UEM Integrations**.

Note　　By default, the **Query Multiple MDM / UEM Integrations** option is disabled.

Step 3　　Choose one of the following options:

- **Endpoint is not Registered with the Configured Primary MDM/UEM Server**: Choose this option if you want Cisco ISE to get the compliance information from all the MDM or UEM servers specified in the authorization policy in the following scenarios:

  - The endpoint's registration information is not present in the primary MDM or UEM server.

  - The endpoint is accessing the network for the first time.

  - The endpoint is not saved in Cisco ISE.

  - You do not know the MDM or UEM server to which the endpoint is registered.

  The endpoint association with an MDM server is checked based on the MDM server name condition in the authorization policy.

- **Primary MDM/UEM Server Sends Error/exception Response**: Choose this option if you want Cisco ISE to query the other MDM or UEM servers that are specified in the authorization policy when the primary MDM or UEM server sends an error message, or is not reachable.

Step 4   Click **Save**.

Configure Timeout for the MDM or the UEM Server

Step 1   In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration** > **Network Resources** > **External MDM**.

Step 2   In the **MDM / UEM Integrations** window, check the check box next to the MDM or the UEM server for which you want to change the timeout value.

Step 3   Click **Change Timeout**. This is the **MDM / UEM Device Compliance Timeout** and is the duration for which Cisco ISE waits for a response from the MDM or UEM server after querying that MDM or UEM server.

Step 4   Enter the timeout value in the **Connection Timeout (milliseconds)** field.

Note   The default timeout for an MDM or UEM server is 30000 milliseconds.

Step 5   Click **Change**.

Cisco ISE MDM Support for Microsoft Intune and Microsoft SCCM

- **Microsoft Intune**: Cisco ISE supports Microsoft Intune device management as a partner MDM server to manage mobile devices.

  Configure Cisco ISE as an OAuth 2.0 client application with the Microsoft Intune server managing mobile devices. Cisco ISE gets a token from Azure to establish a session with the Cisco ISE Intune application.

  For information about how Microsoft Intune communicates with a client application, see https://msdn.microsoft.com/en-us/library/azure/dn645543.aspx.

- **Desktop Device Manager (Microsoft SCCM)**: Cisco ISE supports the Microsoft System Center Configuration Manager (SCCM) as a partner MDM server for managing Windows computers.

For performance and scalability information for Microsoft SCCM integrations, see Size and Scale Numbers for Configuration Manager. Microsoft uses Windows Management Instrumentation (WMI) interfaces based on the Component Object Model (COM), which results in scalability limitations.

Microsoft SCCM Workflow

Cisco ISE retrieves information from the Microsoft SCCM server about whether a device is registered. If the endpoint is registered, Cisco ISE checks for its compliance status. The following diagram shows the workflow for devices that Microsoft SCCM manages.

Figure 8: SCCM Workflow
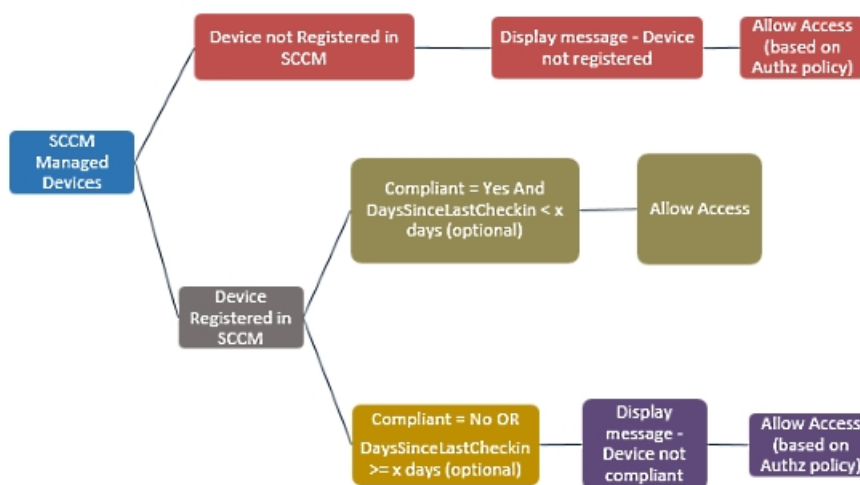
When a device connects to the network and a Microsoft SCCM policy matches, Cisco ISE queries the relevant SCCM server to retrieve compliance and last login (check-in) time. With this information, Cisco ISE updates the compliance status and the lastCheckinTimeStamp of the device in the **Endpoint** list.

If the device is not compliant or not registered with the Microsoft SCCM server, and the authorization policy uses a redirect profile, a message is displayed to the user that the device is not compliant, or is not registered with the Microsoft SCCM. After the user acknowledges the message, Cisco ISE can issue a CoA to the Microsoft SCCM registration site. Users are granted access based on the authorization policy and profile.

Microsoft SCCM Server Connection Monitoring

You cannot configure polling intervals for Microsoft SCCM.

Cisco ISE runs an MDM HeartBeat job that verifies connection with the Microsoft SCCM server, and raises alarms if Cisco ISE loses the connection to the Microsoft SCCM server. The HeartBeat job interval cannot be configured.

Policy Set Example for Microsoft System Center Configuration Manager

The following new dictionary entries are used in policies to support Microsoft SCCM.

- **MDM.DaysSinceLastCheckin**: The number of days since a user last checked in or synchronized a device with Microsoft SCCM. The value may range from 1 to 365 days.

- **MDM.UserNotified**: The valid values are **Y** or **N**. The value indicates whether the user was notified that their device is not registered. You can then allow the user limited access to the network and then redirect them to the registration portal, or deny them access to the network.

- **MDM.ServerType**: The valid value is **MDM** for MDM servers and **DM** for desktop device management.

The following is an example of a policy set that supports Microsoft SCCM.

Policy Name	If	Then
SCCM_Comp	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceRegisterStatus EQUALS Registered	PermitAccess
SCCM_NonComp_Notify	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:UserNotified EQUALS 28	PermitAccess
SCCM_NonComp_Days	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:MDMDeviceCompliantStatus EQUALS Registered AND MDM:DaysSinceLastCheckin EQUALS 28	SCCMRedirect
SCCM_NonComp	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:DeviceRegisterStatus EQUALS Registered	SCCMRedirect
SCCM_UnReg_Notify	Wireless_802.1X AND MDM:DeviceRegisterStatus EQUALS Registered AND MDM:UserNotified EQUALS Yes	PermitAccess

Configure the Microsoft System Center Configuration Manager Server for Cisco ISE

Cisco ISE communicates with the Microsoft SCCM server using Windows Management Instrumentation (WMI). Configure WMI on the Windows server running Microsoft SCCM.

Note The user account that you use for Cisco ISE integration must either:

- Be a member of the SMS Admins user group.

- Have the same permissions as the SMS object under the WMI namespace:

  `root\sms\site_<sitecode>`

  where *sitecode* is the Microsoft SCCM site.

Set Permissions when Microsoft Active Directory Users are in Domain Admin Group

For Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2, the Domain Admin group does not have full control of certain registry keys in the Windows operating system by default. The Microsoft Active Directory administrator must give the Microsoft Active Directory user full control permissions on the following registry keys:

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

The following Microsoft Active Directory versions require no registry changes:

- Windows 2003

- Windows 2003R2

- Windows 2008

To grant full control, the Microsoft Active Directory admin must first take ownership of the key:

Step 1 Right-click the key icon and choose the **Owner** tab.

Step 2 Click **Permissions**.

Step 3 Click **Advanced**.

Permissions for Microsoft Active Directory Users Not in Domain Admin Group

For Windows Server 2012 R2, give the Microsoft AD user full control permissions on the following registry keys:

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

Use the following commands in Windows PowerShell to check if full permission is given to the registry keys:

- ```
  get-acl -path
  "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}"
  | format-list
  ```

- ```
  get-acl -path
  "hklm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" |
  format-list
  ```

The following permissions are required when a Microsoft AD user is not in the Domain Admin group, but is in the Domain Users group:

- Add registry keys to allow Cisco ISE to connect to the domain controller.
- Permissions to Use DCOM on the Domain Controller
- Set Permissions for Access to WMI Root and CIMv2 Namespace, on page 60

These permissions are only required for the following Microsoft AD versions:

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

Add Registry Keys to Allow Cisco ISE to Connect to the Domain Controller

You must manually add some registry keys to the domain controller to allow Cisco ISE to connect as a domain user, and retrieve login authentication events. An agent is not required on the domain controllers or on any machines in the domain.

The following registry script shows the keys to add. You can copy and paste this into a text file, save the file with a .reg extension, and double click the file to make the registry changes. To add registry keys, the user must be an owner of the root key.

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "
```

Make sure that you include two spaces in the value of the DllSurrogate key. If the registry is manually updated, you must include only the two spaces and do not include the quotes. While updating the registry manually, ensure that quotes are not included for AppID, DllSurrogate, and its values.

Retain the empty lines as shown in the preceding script, including the empty line at the end of the file.

Use the following commands in the Windows command prompt to confirm if the registry keys are created and have the correct values:

- `reg query "HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e`

- `reg query HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`

- `reg query HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`

Permissions to Use DCOM on the Domain Controller

The Microsoft Active Directory user who is used for Cisco ISE Passive Identity service must have the permissions to use DCOM on the domain controller server. Configure permissions with the **dcomcnfg** command line tool.

Step 1 Run the **dcomcnfg** tool from the command line.

Step 2 Expand `Component Services`.

Step 3 Expand **Computers** > **My Computer**.

Step 4 Choose **Action** from the menu bar, click **Properties**, and click **COM Security**.

Step 5 The account that Cisco ISE uses for both access and launch must have Allow permissions. Add the Microsoft Active Directory user to all the four options, **Edit Limits** and **Edit Default** for both **Access Permissions** and **Launch and Activation Permissions**.

Step 6 Allow all local and remote accesses for both **Access Permissions** and **Launch and Activation Permissions**.

Figure 9: Local and Remote Accesses for Access Permissions
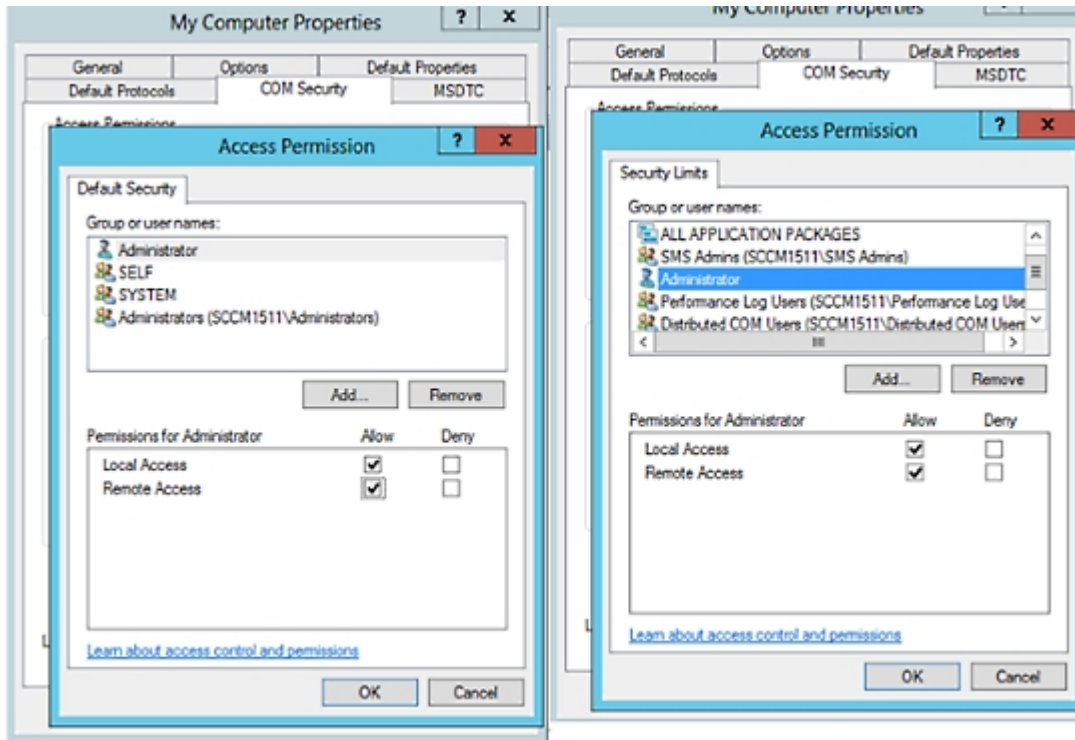
Figure 10: Local and Remote Accesses for Launch and Activation Permissions
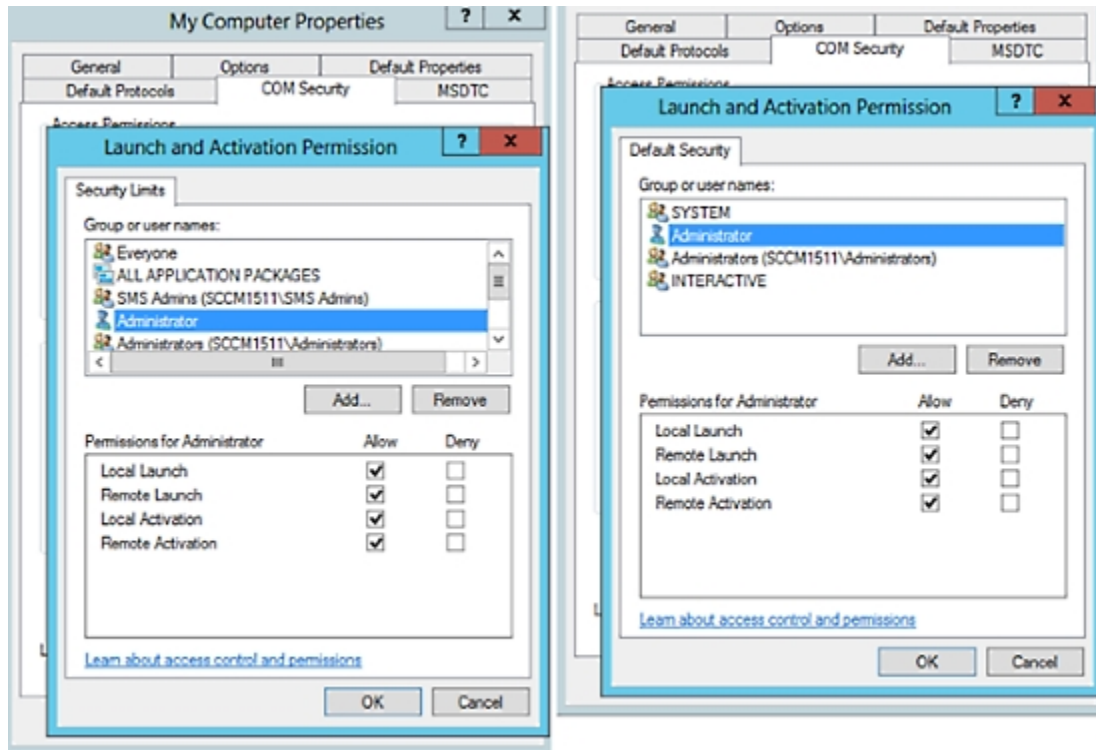
Set Permissions for Access to WMI Root and CIMv2 Namespace

By default, Microsoft Active Directory users do not have permissions for the Execute Methods and Remote Enable. You can grant access using the wmimgmt.msc MMC console.

Step 1   Choose **Start** > **Run** and enter wmimgmt.msc.

Step 2   Right-click **WMI Control** and click **Properties**.

Step 3   Under the **Security** tab, expand **Root** and choose **CIMV2**.

Step 4   Click **Security**.

Step 5   Add the Microsoft Active Directory user, and configure the required permissions as shown in the following image.
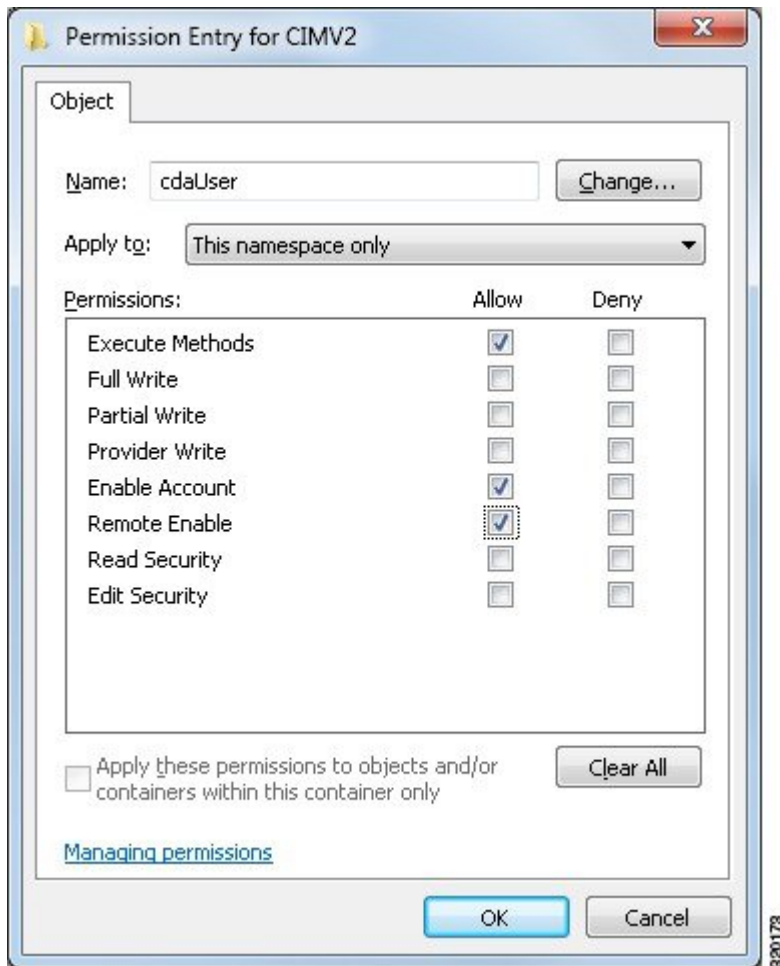
Open Firewall Ports for WMI Access

The firewall software on the Microsoft Active Directory domain controller may block access to WMI. You can either turn off the firewall, or allow access on a specific IP address (Cisco ISE IP address) to the following ports:

- TCP 135: General RPC Port. When performing asynchronous RPC calls, the service listening on this port tells the client which port the component servicing this request is using.

- UDP 138: NetBIOS Datagram Service

- TCP 139: NetBIOS Session Service

- TCP 445: Server Message Block (SMB)

✎

Note   Cisco ISE supports SMB 2.0.

Higher ports are assigned dynamically, or you can configure them manually. We recommend that you add *%SystemRoot%\System32\dllhost.exe* as a target. This program manages ports dynamically.

All firewall rules can be assigned to a specific IP address (Cisco ISE IP).

Select Configuration Baseline Policies for Endpoint Compliance from Desktop Device Manager Server

You can view the baseline policies available in a Desktop Device Manager server (for example, a Microsoft SCCM server) added to Cisco ISE, and choose specific baseline policies to check for endpoint compliance for network access. The configuration baseline policies that are enabled and deployed in the Desktop Device Manager server can be viewed in the Cisco ISE administration portal.

Note Check your user privileges in your desktop device management server to ensure you have the required security permissions to allow baseline policies and compliance information to be sent to Cisco ISE. An administrator must be added in the **Security > Administrator Users** folder of the desktop device manager.

To view the baseline policies in a Desktop Device Manager server in the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration** > **Network Resources** > **External MDM** > **MDM Servers**.

Add a New Desktop Device Manager Server to Cisco ISE, and Select Configuration Baseline Policies

1. In the **MDM Servers** window, click **Add**.

2. Choose **Desktop Device Manager** from the **Server Type** drop-down list.

3. Enter the required details for the following fields:

   • **Host Name / IP Address**: Enter the hostname or IP address of the Microsoft SCCM server.

   • **Instance Name**: If the Microsoft SCCM server has several instances, enter the instance that you want to connect to.

   • **Username**: Enter the username that must be used to connect to the Microsoft SCCM server.

   • **Password**: Enter the password that must be used to connect to the Microsoft SCCM server.

   • **Time Interval For Compliance Device ReAuth Query**: When an endpoint is authenticated or reauthenticated, Cisco ISE uses a cache to get the MDM variables for that endpoint. If the age of the cached value is higher than the value configured in this field, Cisco ISE sends a new device query to the MDM server to get new values. If the compliance status has changed, then Cisco ISE triggers the appropriate CoA.

     The valid range is from 1 to 10080 minutes. The default value is one minute.

4. Choose **Enabled** from the **Status** drop-down list.

To verify that the server is connected to Cisco ISE, click the **Test Connection** button. To view the configuration baseline policies available in this server, click **Save & Continue**. A new window is displayed with a list of names and IDs of the baseline policies.

Select Configuration Baseline Policies from an Existing Desktop Device Manager Server

In the **MDM Servers** window, check the check box for the desired server and click **Edit**. Click the **Configuration Baselines** tab for the list of the baseline policies available in this server.

By default, all the baseline policies are selected. Uncheck the check box next to **Name** to deselect all the baseline policies. Select the required baseline policies by checking the check boxes next to their names. Click **Save**.

Endpoint compliance is checked based on the selected configuration baseline policies.

If there are any changes in the configuration baseline policies in a Desktop Device Manager server, click the **Update Now** button in the **Configuration Baselines** tab for the changes to be updated in Cisco ISE.

Configure Device Identifiers for Windows Endpoints

A Desktop Device Manager server uses certain attributes as identifiers to verify endpoints connecting to the network. The endpoint MAC address is the most popularly used identifier. However, MAC addresses are not the most reliable identifiers when dongles, docking stations, or MAC address randomization techniques are in use.

You can now choose to use hostnames as identifiers. The hostnames are derived from common name (CN) or SAN-DNS attributes available in certificates. Certificate-based authentication of endpoints is mandatory to check for baseline policy compliance using hostnames.

To configure device identifiers for a Desktop Device Manager server, go to its **Server Configuration** tab. From the main menu, choose **Administration** > **Network Resources** > **External MDM** > **MDM Servers** > **Edit**.

In the **Device Identifier Configurations** section, the following identifiers are enabled by default, in this order:

1. **Legacy MAC Address**

2. **Cert – CN, Hostname**

3. **Cert – SAN-DNS, Hostname**

To deselect an identifier, uncheck the check box against the identifier. You can drag the attributes to rearrange the order in which the server must use them for verification.

Verify Configuration of Device Identifiers

When hostnames are used for verification, a GUID is assigned to the endpoint by Cisco ISE. See the **Live Logs** window (In the Cisco ISE GUI, click the **Menu** icon (≡) and choose**Operations** > **RADIUS** > **Live Logs**), and check the GUID entry for details.

Configure an Authorization Profile for Redirecting Nonregistered Devices

You must configure an authorization profile in Cisco ISE to redirect nonregistered devices for each external MDM server.

Before you begin

- Ensure that you have created an MDM server definition in Cisco ISE. Only after you successfully integrate Cisco ISE with the MDM server is the MDM dictionary populated. You can then create an authorization policy using the MDM dictionary attributes.

- Configure ACLs on the Cisco WLC for redirecting unregistered devices.

- If you are using a proxy for Internet connection and the MDM server is part of the internal network, then you have to put the MDM server name or its IP address in the Proxy-Bypass list. In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration** > **System** > **Settings** > **Proxy** to perform this action.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles** > **Add**.

Step 2 Create an authorization profile for redirecting nonregistered devices that are not compliant or registered.

Step 3 Enter a name for the authorization profile that matches the MDM server name, in the **Name** field.

Step 4 Choose **ACCESS_ACCEPT** from the **Access Type** drop-down list.

Step 5 In the **Common Tasks** section, check the **Web Redirection** check box and choose **MDM Redirect** from the drop-down list.

Step 6 Choose the name of the ACL that you configured on the wireless LAN controller from the **ACL** drop-down list.

Step 7 Choose the MDM portal from the **Value** drop-down list.

Step 8 Choose the MDM server that you want to use from the **MDM Server** drop-down list.

Step 9 Click **Submit**.

What to do next

Configure Authorization Policy Rules for the MDM Use Cases

Configure authorization policy rules in Cisco ISE to complete the MDM configuration.

Before you begin

- Add the MDM server certificate to the Cisco ISE certificate store.

- Ensure that you have created the MDM server definition in Cisco ISE. Only after you successfully integrate Cisco ISE with the MDM server does the MDM dictionary get populated, and you can create an authorization policy using the MDM dictionary attributes.

- Configure ACLs on the Cisco WLC for redirecting unregistered or noncompliant devices.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Policy** > **Policy Sets**, and expand the policy set to view the authorization policy rules.

Step 2 Add the following rules:

- **MDM_Un_Registered_Non_Compliant**: For devices that are not yet registered with an MDM server or noncompliant with MDM policies. When a request matches this rule, the Cisco ISE MDM window is displayed to a user, with information on registering the device with the MDM server.

Note   Do not use the **MDM.MDMServerName** condition in this policy. When this condition is used, an endpoint matches the policy only if the endpoint is registered with the MDM server.

- **PERMIT**: If the device is registered with Cisco ISE, registered with MDM, and is compliant with Cisco ISE and MDM policies, it is granted access to the network based on the access control policies configured in Cisco ISE.

Step 3   Click **Save**.

Configure ACLs on Wireless Controllers for MDM Interoperability

Configure ACLs on the Wireless Controller for use in an authorization policy to redirect nonregistered devices and certificate provisioning. Your ACLs must be in the following sequence.

Step 1   Allow all outbound traffic from the server to the client.

Step 2   (Optional) Allow ICMP inbound traffic from the client to the server for troubleshooting.

Step 3   Allow access to the MDM server for unregistered and noncompliant devices to download the MDM agent and proceed with compliance checks.

Step 4   Allow all inbound traffic from the client to the server to Cisco ISE for the web portal and supplicant, and certificate provisioning flows.

Step 5   Allow inbound Domain Name System (DNS) traffic from the client to the server for name resolution.

Step 6   Allow inbound DHCP traffic from the client to the server for IP addresses.

Step 7   Deny all inbound traffic from the client to the server to corporate resources for redirection to Cisco ISE (as per your company policy).

Step 8   (Optional) Permit the rest of the traffic.

Example

The following example shows the ACLs for redirecting a nonregistered device to the BYOD flow. In this example, the Cisco ISE IP address is 10.35.50.165, the internal corporate network IP addresses are 192.168.0.0 and 172.16.0.0 (to redirect), and the MDM server subnet is 204.8.168.0.

Figure 11: ACLs for Redirecting Nonregistered Device

Wipe or Lock a Device

Cisco ISE allows you to wipe or enable a pin lock for a lost device. You can configure this from the **Endpoints** window.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Work Centers** > **Network Access** > **Identities** > **Endpoints**.

Step 2 Check the check box next to the device that you want to wipe or lock.

Step 3 From the **MDM Actions** drop-down list, choose one of the following options:

- **Full Wipe**: Depending on the MDM vendor, this option either removes the corporate apps or resets the device to the factory settings.

- **Corporate Wipe**: This option removes applications that you have configured in the MDM server policies.

- **PIN Lock**: This option locks the device.

Step 4 Click **Yes** to wipe or lock the device.

View Mobile Device Management Reports

Cisco ISE records all additions, updates, and deletions of MDM server definitions. You can view these events in the **Change Configuration Audit** report, which displays all the configuration changes from any system administrator for a selected time period.

In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Operations** > **Reports** > **Reports** > **Audit** > **Change Configuration Audit**. Check the entries in the **Object Type** and **Object Name** columns for the MDM server that you want to review, and click the corresponding **Event** value to view the details of the configuration event.

View Mobile Device Management Logs

You can use the **Debug Wizard** window to view mobile device management log messages. In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Operations** > **Troubleshoot** > **Degug Wizard** > **Debug Log Configuration**. Click the radio button next to a Cisco ISE node and click **Edit**. In the new window displayed, click the radio button next to the component name **external-mdm**, and click **Edit**. The default log level for this component is **INFO**. Choose **DEBUG** or **TRACE** from the corresponding **Log Level** drop-down list, and click **Save**.
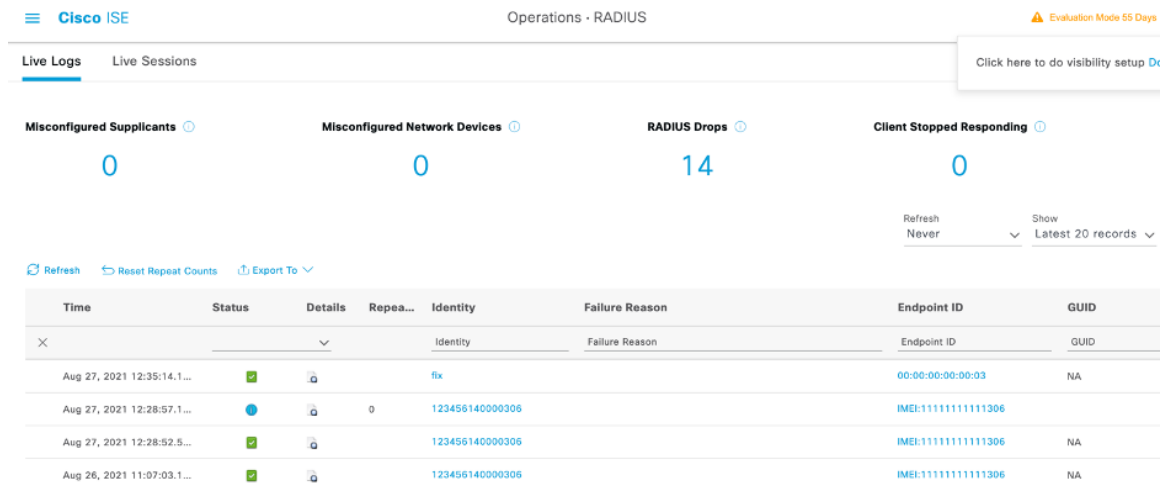
Configure Cisco Private 5G as a Service

From Cisco ISE Release 3.2, Cisco ISE supports Cisco Private 5G and Session Management Function (SMF) software. Cisco ISE provides policy configuration for 5G authorization, that is implemented with RADIUS authorize-only and accounting flows. Communication with the SMF happens with the help of RADIUS protocol. Communication between Cisco ISE and Cisco Private 5G happens with the help of OpenAPI and ERS APIs.

Before you begin

You must have Cisco Private 5G deployed in your network, before enabling it as a service in Cisco ISE.

Step 1 Configure Cisco ISE as a RADIUS server on the Cisco Private 5G on-prem Cisco ISE proxy.

Step 2 Enable ERS and Open APIs.

After you enable the ERS and Open APIs, you can perform the subsequent steps using APIs or from the Cisco ISE GUI.

Step 3 Enable 5G in Cisco ISE:

a) In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Policy** > **Policy Elements** > **Results** > **Authentication** > **Allowed Protocols**.

b) Add a new **Allowed Protocols** service or modify an existing one.

Note It is not mandatory to create a new service. You can use the existing **Default Network Access** service for the 5G endpoints as well.

c) Modify the settings according to your network requirement.

d) Check the **5G** check box.

e) Click **Save**.

For example, you can create the **Allowed Protocols Services that are shown** in the following figure to match the 5G traffic:

Figure 12: Allowed Protocols Services for 5G

Step 4   Configure SMF as a network device in Cisco ISE.

Step 5   Create a new identity group or use an existing one. 5G users are stored as subscribers in the Cisco ISE internal database.

Step 6   Create User Identity Groups or choose from any of the default user identity groups in Cisco ISE.

Step 7   Create a new policy set or use an existing policy.

The **Network Access.UseCase** attribute in **Conditions Studio** is populated with the new value, **FiveG**. You can now build policies based on the **UseCase** attribute as well.

Figure 13: UseCase Attribute Location in Condition Library

A new built-in condition, **5G**, is also available in the **Library** in **Conditions Studio**. This condition uses the **Cisco·Cisco-5g-serving-network-name** attribute that can be used to match 5G endpoints.

Figure 14: 5G Condition
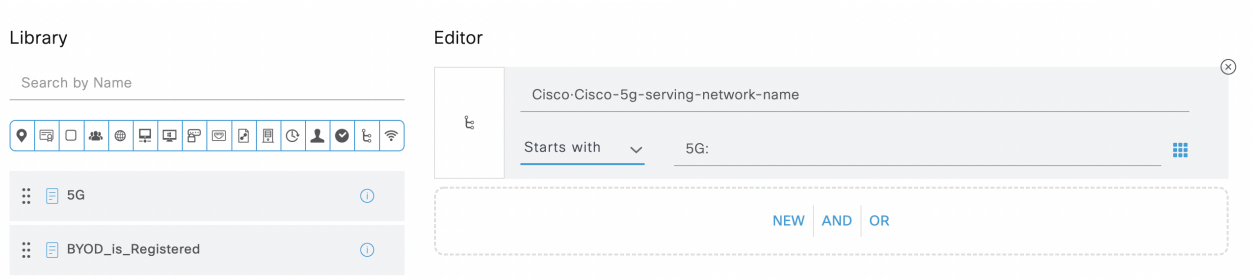
You can push the allowed protocols service profile that you created earlier, for this policy.

Figure 15: Policy Set for 5G

Step 8   Cisco Private 5G uses the 5GaaS APIs to add subscribers (cellular users) and user equipment (mobile devices) in Cisco ISE.

For example, the endpoint identity group shows the added subscribers, as displayed in the following figure:

Figure 16: Endpoint Identity Group for 5G Subscribers

You can check the **Live Logs** and **Live Sessions** to view the 5G session logs and troubleshoot when necessary. **Live Sessions** has a new column, **Usecase** (disabled by default), where you can use the filter **5G** to filter the 5G endpoints. You can also use the prefix **IMEI:** in the **Endpoints** column to filter 5G endpoints.

Figure 17: 5G Live Logs

Figure 18: 5G Live Sessions

Configure Cisco Private 5G as a Service

From Cisco ISE Release 3.2, Cisco ISE supports Cisco Private 5G and Session Management Function (SMF) software. Cisco ISE provides policy configuration for 5G authorization, that is implemented with RADIUS authorize-only and accounting flows. Communication with the SMF happens with the help of RADIUS protocol. Communication between Cisco ISE and Cisco Private 5G happens with the help of OpenAPI and ERS APIs.

Before you begin

You must have Cisco Private 5G deployed in your network, before enabling it as a service in Cisco ISE.

Step 1 Configure Cisco ISE as a RADIUS server on the Cisco Private 5G on-prem Cisco ISE proxy.

Step 2 Enable ERS and Open APIs.

After you enable the ERS and Open APIs, you can perform the subsequent steps using APIs or from the Cisco ISE GUI.

Step 3 Enable 5G in Cisco ISE:

a) In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Policy** > **Policy Elements** > **Results** > **Authentication** > **Allowed Protocols**.

b) Add a new **Allowed Protocols** service or modify an existing one.

Note It is not mandatory to create a new service. You can use the existing **Default Network Access** service for the 5G endpoints as well.

c) Modify the settings according to your network requirement.

d) Check the **5G** check box.

e) Click **Save**.

For example, you can create the **Allowed Protocols Services that are shown** in the following figure to match the 5G traffic:

Figure 19: Allowed Protocols Services for 5G
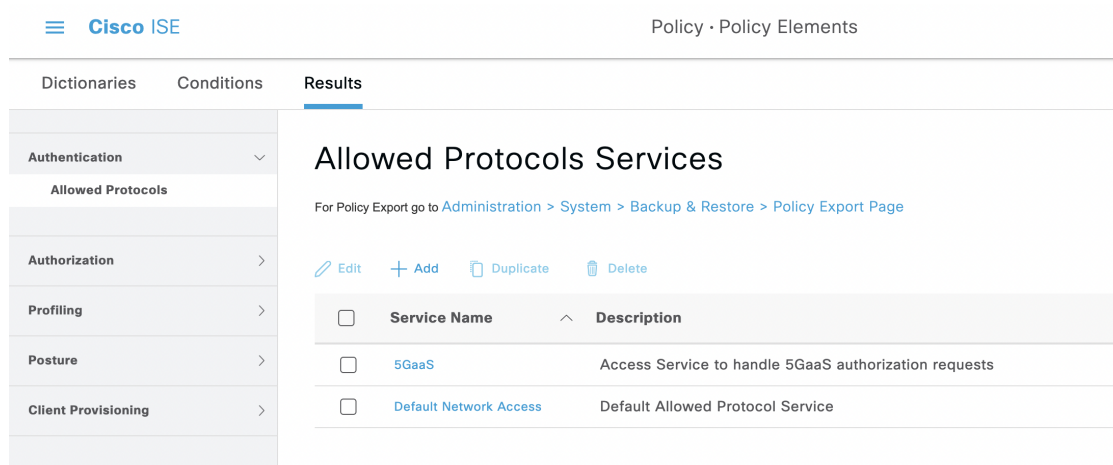
Step 4 Configure SMF as a network device in Cisco ISE.

Step 5 Create a new identity group or use an existing one. 5G users are stored as subscribers in the Cisco ISE internal database.

Step 6 Create User Identity Groups or choose from any of the default user identity groups in Cisco ISE.

Step 7 Create a new policy set or use an existing policy.

The **Network Access.UseCase** attribute in **Conditions Studio** is populated with the new value, **FiveG**. You can now build policies based on the **UseCase** attribute as well.

Figure 20: UseCase Attribute Location in Condition Library
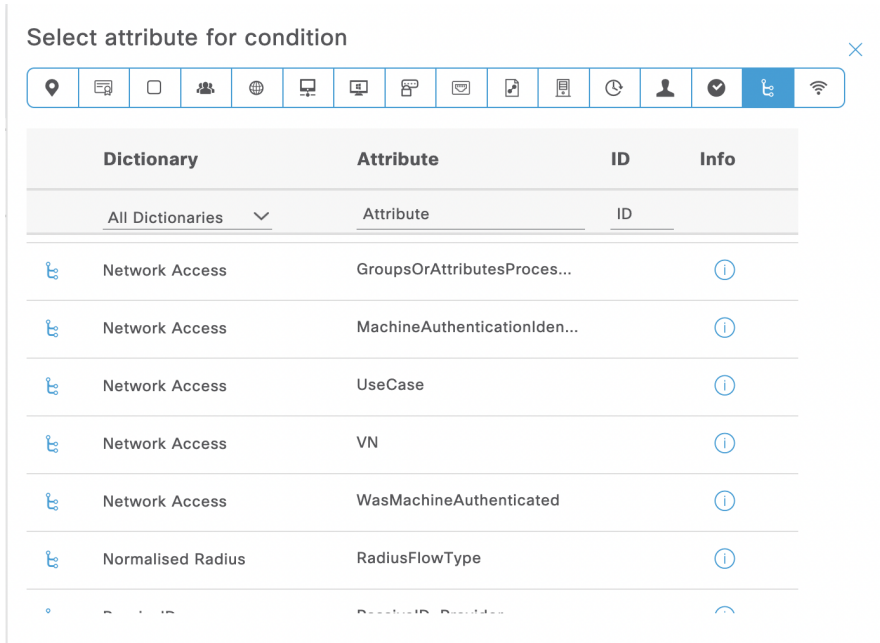
A new built-in condition, **5G**, is also available in the **Library** in **Conditions Studio**. This condition uses the **Cisco·Cisco-5g-serving-network-name** attribute that can be used to match 5G endpoints.

Figure 21: 5G Condition
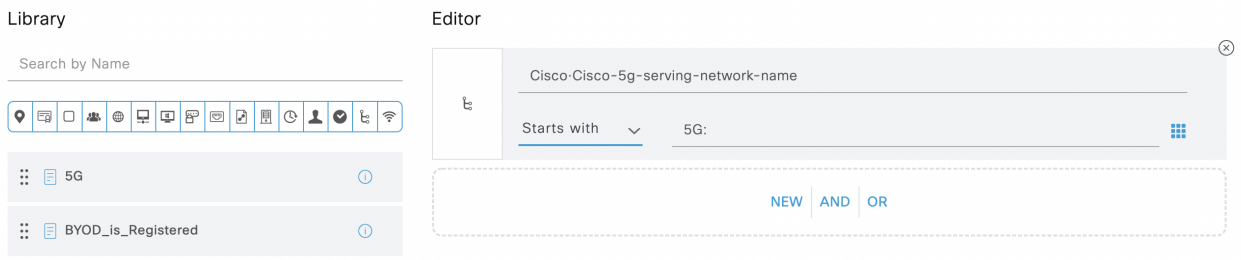
You can push the allowed protocols service profile that you created earlier, for this policy.

Figure 22: Policy Set for 5G
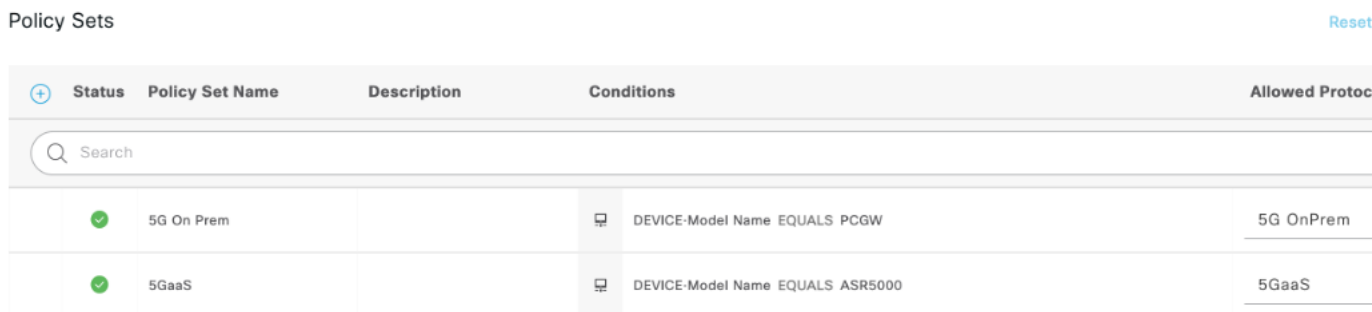
Step 8   Cisco Private 5G uses the 5GaaS APIs to add subscribers (cellular users) and user equipment (mobile devices) in Cisco ISE.

For example, the endpoint identity group shows the added subscribers, as displayed in the following figure:

Figure 23: Endpoint Identity Group for 5G Subscribers

You can check the **Live Logs** and **Live Sessions** to view the 5G session logs and troubleshoot when necessary. **Live Sessions** has a new column, **Usecase** (disabled by default), where you can use the filter **5G** to filter the 5G endpoints. You can also use the prefix **IMEI:** in the **Endpoints** column to filter 5G endpoints.
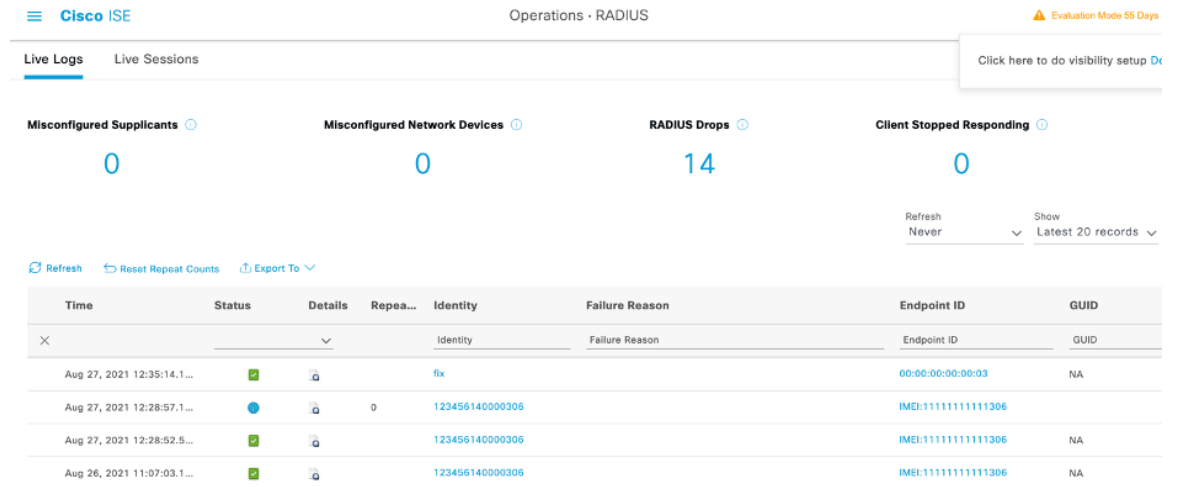
Figure 24: 5G Live Logs

Figure 25: 5G Live Sessions